UNITED STATES SENTENCING COMMISSION

PUBLIC HEARING

TUESDAY, MARCH 17, 2009
AND
WEDNESDAY, MARCH 18, 2009

The public hearing convened in the Federal Judicial Center Training Rooms, in the Thurgood Marshall Building, 1 Columbus Circle, N.E., Washington, D.C. at 2:15 p.m. Tuesday, March 17 and 8:30 a.m. Wednesday, March 18, Ricardo H. Hinojosa, Acting Chair, presiding.

COMMISSIONERS PRESENT:

RICARDO H. HINOJOSA, Acting Chair
WILLIAM B. CARR, JR., Vice Chair
RUBEN CASTILLO, Vice Chair
WILLIAM K. SESSIONS, III, Vice Chair
DABNEY L. FRIEDRICH, Commissioner
BERYL A. HOWELL, Commissioner
EDWARD F. REILLY, JR., Commissioner
JONATHAN WROBLEWSKI, Commissioner

STAFF PRESENT:

JUDITH W. SHEON, Staff
PANELISTS PRESENT:

MICHAEL DUBOSE, Chief, CCIPS, Criminal Division, United States Department of Justice
ERIC HANDY, Mid Atlantic Coast Representative, Identity Theft Resource Center
JENNIFER COFFIN, National Sentencing Resource Counsel, Federal Public and Community Defenders
VINCENT WEAFER, Vice President, Security Response, Symantec
SETH SCHOEN, Staff Technologist, Electronic Frontier Foundation
JOSEPH E. KOEHLER, Assistant United States Attorney, Deputy Chief, Criminal Division Immigration Unit, United States Attorney's Office, District of Arizona
LESLEY WHITCOMB FIERST, Associate, Womble Carlyle Sandridge & Rice, PLLC, Federal Public and Community Defenders
KAREN STAUSS, Managing Attorney and Policy Counsel, Polaris Project
CHARLES SONG, West Coast Pro Bono Director, Howrey LLP
SUZANNE FERREIRA, Supervising United States Probation Officer for the Southern District of Florida; Chair, Probation Officers Advisory Group
CRAIG D. MAGAW, Deputy Assistant Director, Office of Investigations, United States Secret Service
DONNA LEE ELM, Federal Public Defender for the Middle District of Florida, Federal Public and Community Defenders
KENNETH H. LINN, Chairman, FedCURE, Citizens United for Rehabilitation of Errants, Federal Prison Chapter
MICHAEL J. PROUT, Assistant Director for Judicial Security, Judicial Security Division, United States Marshals Service
JON M. SANDS, Federal Public Defender for the District of Arizona, Chair, Federal Defender Sentencing Guidelines Committee
TODD A. BUSSERT, Co-Chair, Practitioners
Advisory Group
ERIK R. STEGMAN, Board of Directors, The Nakwatsvewat Institute; Carry the Kettle First Nation (Assiniboine)
MARIO J. SCALORA, Associate Professor of Psychology, University of Nebraska -Lincoln
TABLE OF CONTENTS

Tuesday, March 17, 2009

Identity Theft and Restitution Act of 2008

Michael DuBose . . . . . . . . . . . . . . .7
Eric Handy . . . . . . . . . . . . . . . 19
Jennifer Coffin . . . . . . . . . . . . . . 27
Vincent Weafer . . . . . . . . . . . . . . 39
Seth Schoen . . . . . . . . . . . . . . . 49
Q&A Session . . . . . . . . . . . . . . . 65

Williams Wilberforce Trafficking Victims Protection Reauthorization Act of 2008

Joseph Koehler . . . . . . . . . . . . . . 99
Leslie Whitcomb Fierst . . . . . . . . .107
Karen Stauss . . . . . . . . . . . . . . . 117
Charles Song . . . . . . . . . . . . . . 123
Q&A Session . . . . . . . . . . . . . . 132

Other Guideline Amendments

Suzanne Ferreira . . . . . . . . . . . . .163
Craig Magaw . . . . . . . . . . . . . . 177
Donna Lee Elm . . . . . . . . . . . . . 185
Kenneth Linn . . . . . . . . . . . . . . 196
Q&A Session . . . . . . . . . . . . . . 204

Wednesday, March 18, 2009

Court Security Improvement Act of 2007

Michael J. Prout . . . . . . . . . . . . .211
Jon Sands . . . . . . . . . . . . . . . 219
Todd Bussert . . . . . . . . . . . . . . 225
Erik R. Stegman . . . . . . . . . . . . 238
Mario Scalora . . . . . . . . . . . . . . 242
Q&A Session . . . . . . . . . . . . . . 250

Adjourn
P-R-O-C-E-E-D-I-N-G-S

(2:28 p.m.)

ACTING CHAIR HINOJOSA: We'll go ahead and get started. First of all, I would like to welcome everyone to the public hearing of the United States Sentencing Commission with regards to the proposed list of possible guidelines and guideline amendments with regards to the 2008 - 2009 cycle. We do appreciate the fact that those of you who have testified have taken up your time to come here and share some thoughts with us.

I cannot emphasize how important the thoughts of the individuals who come to the public hearings are to the Commission with regards to our work and the year-long process of the guideline amendment process, as well as the promulgation of new guidelines. It is part of the process that we use with regards to our statutory mission and part of the process that we use within that mission to determine what guideline amendments and new guidelines should be promulgated under the
3553 factors, as the statute requires us to do.

And, again, on behalf of the entire Commission, and I'll start from my right to my left and introduce all the commissioners whom I'm sure most of you know. Mr. Jonathan Wroblewski is the ex officio member representing the Attorney General. Ms. Beryl Howell is a Commissioner. She practices here in the District of Columbia. Mr. William Carr, Jr., is a Vice Chair of the Commission. He is our newest member of the Commission. He's from Philadelphia.

We also have Vice Chair William Sessions who will be coming in shortly. He is still held up at judicial conference meetings. Vice Chair and Judge Ruben Castillo from Chicago, and Commissioner Dabney Friedrich from here in the District of Columbia. And Commissioner Ed Reilly, who is the ex officio member who is the Chair of the Patrol Commission.

Our first panel will be presenting
their views with regards to the Identity Theft and Restitution Enforcement Act of 2008 issues that we put out for public comment. The first member of the panel is Michael DuBose who is the Chief -- did I get that right?

MR. DUBOSE: Yes.

ACTING CHAIR HINOJOSA: Who is the Chief of the Computer Crime and Intellectual Property Section of the Criminal Division of the Department of Justice. Previously, he has served as Senior Counsel for Enforcement at the Department of Treasury, and he has also served as an Assistant U.S. Attorney in Maine for seven years.

We also have Mr. Eric Handy. He is a volunteer representative for the Identity Theft Resource Center, assisting in educating identity theft victims in the Washington, D.C. area. He serves as a consulting manager with a law firm here in D.C. with regards to their federal security and privacy practice, and they are based in Washington, D.C.
We also have Ms. Jennifer Coffin who is a Staff Attorney for National Sentencing Resource Council of the Federal Public and Community Defenders. Prior to becoming a staff attorney with the Resource Council office, she served as a Research and Writing Specialist for the Office of the Federal Public Defender for the Middle District of Tennessee.

Mr. Vincent Weafer is a Vice President for Symantec Security Response, where he is responsible for advancing research into new computer security threats and for providing security content solutions. He is also a co-author with regards to a book on internet security.

We have Mr. Seth Schoen, who is a Staff Technologist for the Electronic Frontier Foundation where he assists other technologists to understand technology -- I might talk to you afterwards -- and technology products and the civil liberty implications related to the use of technology.
Each one of the witnesses has been told that they have seven minutes, and then that would leave enough time for questions and answers. We are starting a little bit late because of the judicial conference, but we'll go ahead and start with Mr. DuBose.

MR. DUBOSE: Thank you, Chairman Hinojosa. Distinguished members of the Commission, thank you for inviting the Department of Justice to present testimony today on the Identity Theft Restitution and Enhancement Act of 2008. In light of the time constraints, I will not try to address every option or proposal that was set forth in the Commission's proposed amendments published in last January. Instead, I'll focus on a more limited number of issues, recognizing that, as customary, we'll be submitting a more detailed letter in a few days.

Before addressing the specific proposals, I would first like to describe how the landscape of cybercrime and identity theft has changed since this Commission last visited.
these issues in 2003. At that time, the Commission cited data in its report to Congress indicating that crime prosecuted under 18 USC Section 1030 was "relatively unsophisticated." Much has changed since then. Cyber criminals and identity thieves have become more sophisticated in concealing their identities and locations from law enforcement, often using proxy technologies to route their communications through dummy computers connected to the internet which serve to mask the true origin of their transmissions.

Moreover, in recent years, investigators and prosecutors have been fighting the rising threat of botnets, the term used to describe networks of computers infected by malicious software and highjacked by hackers without the knowledge or consent of their owners. Botnets can range in size from thousands up to hundreds of thousands of infected computers. Computers compromised in this way can not only be used as proxies but
also can be used to carry out so-called 
fishing scams and also are used in numerous 
denial-of-service attacks on targeted computer 
systems.

In addition to increased 
technological sophistication, one of the most 
worrysome trends that we're also seeing is the 
increased commercialization of cybercrime. 
Theft of information is now big business. 
Cyber criminals trafficking stolen information 
employ a sophisticated division of labor that 
spans the globe. The synergy between rapid 
technological advancement and enormous 
financial gain has resulted in an explosion in 
cybercrime since the Commission last visited 
this issue in 2003.

As Senator Leahy noted when the 
Senate passed the ID Theft Act, the FTC 
reported that identity theft was the fastest-
growing crime in 2008, affecting 10 million 
Americans. Indeed, Consumer Reports recently 
reported the United States experiences roughly 
30 percent of all malicious cyber activity in
the world and that Americans face a one-in-four chance of becoming a victim of cybercrime.

The ID Theft Act was passed in response to this changing landscape. Seeking to provide more effective prosecution of identity theft and cybercrime offenses, the Act directed the Sentencing Commission to amend the guideline for these crimes "in order to reflect the intent of Congress that such penalties be increased in comparison to those currently provided."

With that congressional intent in mind, I would now like to turn to several of the Commission's proposals that are of particular, though not exclusive, interest to the Department of Justice. First, the Department of Justice strongly supports the Commission's January proposal to amend Application Note 8(b) to Section 2(b)1.1, which provides that in a scheme involving computers "the use of any software or technology to conceal the identity or
geographic location of the perpetrator ordinarily indicates sophisticated means."

As I noted in my testimony last November and in my opening today, there has been a significant rise in the use of proxy computers by cyber criminals to hide their identities and evade prosecution. The Commission's proposal uses technology-neutral language to clarify that the use of proxies should normally qualify as a sophisticated means, thereby providing a more effective deterrent to this conduct and encouraging uniform sentencing treatment among all the districts.

Next, I'd like to address the Commission's response to the ID Theft Act's concern over whether the guidelines adequately address the loss resulting from the theft of two specific types of information: first, information that the victim retains but which is copied by a defendant; and, second, information that constitutes a trade secret or other proprietary information. Of the two
options put forth by the Commission for comment, the Department strongly supports option number two and not option one. First, option two would amend Application Note 3(C) to permit courts to consider the fair market value of information where the information is copied and where the owner is not, in fact, deprived of its use.

Currently, the application note refers only to property "taken or destroyed," thus leaving ambiguous whether the fair market value of information that is merely copied may be used to calculate loss. It's important to remove this ambiguity because the theft of information usually does involve copying of the information, and its fair market value is an appropriate measure of the seriousness of the offense regardless of whether the owner is actually deprived of its use or not.

Option two is also preferable because its application is not limited only to Section 1030 offenses, like option one is, but rather applies to a broader cross-section of
offenses and, in particular, trade secret cases prosecuted under 18 USC Sections 1831 and 1832. Finally, option two is the better of the two options because it gives courts greater flexibility in calculating loss for offenses involving the theft of information. Whereas option one is limited to considering only the reduction in value to the proprietary information, option two permits courts to consider fair market value, the cost of development or the diminution in value to the information that resulted from the offense. This more flexible approach is also more in line with existing precedent, as courts have already used fair market value and development costs when estimating loss in theft of information cases.

I would next like to turn to the Commission's request for comment on whether a defendant's intent to cause damage and intent to obtain personal information should be disaggregated and considered separately from other factors in Section 2(b)1.1, Subsection
(b)15. We think they should. As it currently is structured, Subsection (b)15 can result in strikingly similar sentences for dissimilar conduct. For instance, a hacker with the intent to obtain information from an individual's home computer would receive the exact same two-level enhancement as one who steals that information by hacking into a computer that is part of a critical infrastructure. Similarly, someone who intentionally damages a military computer would receive the same four-level increase as one who damages a single home computer. And an individual who accidentally causes a substantial disruption to a critical infrastructure computer receives the same six-level enhancement as one who intentionally does so.

The failure to account for these differences in offense severity and culpability frustrates the goal of proportional and fair punishment. The Department believes that this problem can be
and should be fixed by simply separating the
factors in Section 2(b)115 (b)15 and allowing
them to apply independently and cumulatively
as the offense conduct dictates. Let me also
be clear, however, the Department does not
believe that the scope of Section 2(b)115
(b)15 should be expanded to apply to crimes
other than Section 1030 offenses.

Finally, I would like to respond
to the Commission's request for comment on
whether aggravated offense conduct involving
the disclosure of personal information is
adequately addressed by the guidelines. The
Department believes that the disclosure of
private information to the public almost
always increases the significance of the
original privacy invasion. As I hope my
testimony last November made clear, illegally
copying the medical records of Tammy Wynette
for one's personal interest without sharing
that information with anyone else is
qualitatively different than copying those
same records and selling them to a tabloid for
national publication or posting those medical records on the internet for all to see.

Accordingly, the Department strongly supports adoption of a proposal that would provide a two-level enhancement for disclosures of personal information which the defendant knew, intended, or had reason to believe would cause a risk of substantial non-monetary harm. For purposes of making this determination, we believe the definition of personal information in Application Note 13(a) is sufficient.

This concludes my prepared remarks. Thank you again for inviting the Department to testify about these important issues, and we remain ready to assist you in any way going forward. Thank you.

ACTING CHAIR HINOJOSA: Thank you, Mr. DuBose. Mr. Handy, sir?

MR. HANDY: Good afternoon, everyone, Committee. It's a pleasure to be here, first of all. It's an honor to be here representing the Identity Theft Resource
Center, first of all. And I just want to --
we're going to focus, for the most part, on
the scenarios, scenario A and scenario B.
Basically, scenario A was that the hacker
steals personal information from a computer
just because they can but has no intent on
using it. At that point, no one suffers a
loss. That's scenario A.

Scenario B is that the hacker
steals personal information from a computer
with the intent of selling or using it to
steal identities. Businesses suffer at a
loss, ID victims suffer a loss.

The question that was proposed for
us is should these be the same, or should they
be different? Our response is that these
should be the same, and this is the reason why
they should be the same, in our estimation.

Businesses must report all breach
notifications. Forty-four of the states have
breach notification laws, as most of us
probably know. And because of that, if
someone wants to breach any network that will
be probably reported, has to be reported, obviously, and exposures that have to be reported. In that particular case, there is a victim in that case. The victim is the business. Even if nothing happens and, say, supposedly no one's identity is breached, there is still an issue because the businesses, at that point, have to notify everyone.

Now, let's take the VA situation a couple of years ago where 26.5 million people's identities were supposedly exposed and you had to notify all those people. Just think about the postage alone, how much it costs just to send the postage to notify these folks that they may have been breached and the envelopes and so on and so on. Just looking at the stamps alone, it's over $10 million if you add it up, but, yet, we don't have a victim supposedly here in that situation.

So we beg to differ that there is a victim in that particular situation. There's all sort of business costs. Each
record statistically, if you look at some of
the statistics, cost anywhere from $182 to
$128 to rectify if someone is breached.

Also, if you look at it, in a lot
of cases any identity theft worth its salt, in
a lot of cases they have Social Security
numbers, are not going to use them initially,
so it's going to appear that there is no
theft, obviously, at that point. But they're
going to wait until after the credit
monitoring services are given out, which is
another expense that businesses have to incur.
There's attorney fees, of course. There's
accounting issues. A lot of background costs
that we don't really associate sometimes with
breaches will come up for the businesses. So
this is very costly, especially in this day in
time of economics and the economy. We don't
want the businesses having to pay out these
kind of expenses unnecessarily.

Therefore, that's why we want both
of these measures, both of these sentences
should be the same in that particular case.
And they need to be within the enforcement within the sentencing. It's just not enough just to have a high sentence, but you also need to enforce it in order for it to be effective, in our viewpoint. But that's what we are recommending.

Again, there's also a victim potentially involved in this, as well. So there's always going to be a business element that's going to be a cost factor, but if there is a breach and there it is exposure, and in a lot of cases they're starting to come up to be exposures. Look at the TJ Maxx situation that came out. There were exposures there that they ended up finding people actually using those card datas.

Also, we have the criminals are getting smarter, obviously. We all know that. But the thing that's really scary is that people are actually looking at the card system, such as Heartland. Now, I'm sure some of us in this room, I'm included, received a letter about Heartland and that I could have
potentially been one of those 560,000 people that has been exposed. And I'm always getting hit by these things for some reason. I never win the lottery, I never win the raffles. Even in my little league son's team I never win those lottos, I never win those raffles. I don't know why. But I always get hit with these things.

So a lot of people are getting hit with these things all the time, so we just need to address it. And that's why we just can't take this lightly. People need to think twice before breaking into a network.

Now, let's look at the victim side of it because we deal with the victims, obviously, at the Identity Theft Resource Center. And Nicole, who was supposed to be here today but she, unfortunately, is not feeling well, she's been dealing with identity theft for eight years. I don't know if some of you know her or not, eight or ten years trying to fix the problem. And when her imposter was caught, they still continued to
hurt her even while in jail, even while on
probation because the sentencing wasn't really
anything that really bothered the person. So
we're really concerned with the sentencing
piece of this and make sure that people need
to think twice before they commit this sort of
crime because it will go far deeper than no
one getting hurt.

When I looked at this initially,
this scenario reminded me of the old middle
school science class project that you hear
sometimes where if the tree falls in the
forest no one hears it, no one is there, it
doesn't make a sound. In this case, if
someone breaks into a network but no harm is
done supposedly, who's your victim is the
question. And in this case, there is a
victim, and that is the business, at least;
and there may be even some other consumer
victims, as well, to address.

We also are concerned about
vigilante behavior out there where people are
going out and breaking into systems just to
prove that they can. And we still think that's dangerous because, as I just mentioned before, there's so many business costs that kick in for the business when they have to notify people, so much that's going to go into this that we just want to make sure that that is accounted for in that first scenario, that there will be some costs, even if you don't hear anything. And not to mention, we haven't gotten to the point yet where we really know what happens three or four years down the road after all the prevention measures, after people get lax again with prevention. What's really happening out there with the criminals?

I've done some research on some prospective identities of criminals, and they hold that information, obviously, for long periods of time because they know if they do it right away it won't help. If you have a Social Security number, you know it's better to hold it because everyone is looking at their credit monitoring and other materials. Now, if you have a credit card, obviously you
want to strike right away because that is a limited function.

Bottom line is that both these sentences should be the same. And because these sentences will probably be complicated anyway, there should be added measures to some of the more severe cases. But I can't underestimate, you know, I have a lot of statistics to give you that I can give you more, and you'll hear statistics the rest of the day, but the thing that we know the most is the victims. We hear the victims everyday, and those victims' voices speak loud and clear that this is a big problem that we all need to address.

I'd like to thank everyone for their time, and it's much appreciated. And we'll answer questions later. Thank you very much.

ACTING CHAIR HINOJOSA: Thank you, Mr. Handy. Ms. Coffin?

MS. COFFIN: Judge Hinojosa and members of the Commission, thank you very much
for the opportunity to testify on behalf of
the Federal Public and Community Defenders.
I submitted lengthy written testimony
addressing in some detail a number of issues
relating to Congress' directive in Section 209
of the Identity Theft Enforcement and
Restitution Act of 2008. The Defenders firmly
believe that the guidelines are adequate and,
in some cases, greater than necessary for
offenses involving computers and identity
theft and that the Commission should not
increase punishment.

I would like to focus my comments
today on a couple of key areas that we believe
deserve special attention as the Commission
moves forward in responding to this directive.
First and perhaps most important is the
question of deterrence. The Commission has
proposed a number of changes to the
guidelines, each of which will have the effect
of increasing the recommended punishment for
offenses involving computers and the misuse of
identifying information. The Department of
Justice, by and large, supports these proposals and it sounds like has added a few of its own on the apparent theory that guideline ranges are not high enough. But no one seems to be addressing, I mean really addressing the fundamental aim of Congress' directive, which is presumably why we're here today.

Congress directed the Commission to study the extent to which the guidelines may or may not account for 13 specified factors in the context of five statutes and then in determining the appropriate guideline range for these offenses to "create an effective deterrent to computer crime and the theft or misuse of personally-identifying information." Thus, the very first question that should be asked and answered with respect to any proposed change is whether there is any evidence that the change will make the guideline a more effective deterrent. But no one seems to be asking that question, let alone answering it.
We have pointed to substantial evidence that increasing guideline ranges would not be an effective deterrent to these offenses. It is worth noting that the original commission explicitly stated that it turned to past practice because, quote, those who subscribe to a philosophy of crime control may acknowledge the lack of sufficient data might make it difficult to determine exactly the punishment that will best prevent that crime. Since that time, the Commission has never identified any evidence that might form the basis for setting or increasing penalty levels to better deter crime. In fact, currently empirical research confirms that it is the certainty of punishment, not its severity, that deters crime.

For white collar offenders in particular, the research shows no difference in deterrence even between probation and prison. Further, Commission data indicate that the offenders to whom this directive is aimed present a low risk of committing future
crimes. Increasing punishment is, therefore, not necessary to prevent future crimes of these defendants.

We recognize that computer crimes and identity theft are a problem and that there may be challenges to law enforcement and prevention, and we understand that many believe that increasing punishment will deter others from committing crimes. But the Commission's mandate is not to make law enforcement easier or to act on beliefs that are unfounded by empirical research.

Congress created the Commission to do what it cannot: to act as an independent expert body to gather evidence and data and to establish sentencing practices that will reflect, to the extent practicable, advancement and knowledge of human behavior as it relates to the criminal justice process. This is the Commission's primary organic purpose.

Because the evidence indicates that increasing punishment will not create an
effective deterrent, the Commission should not act on the erroneous assumption that it will. This would be unsound policy. Instead, the Commission should explain to Congress that increasing punishment will not deter these crimes and that their guideline ranges already adequately take the 13 factors into account. That's what the Commission was created to do, and that's what the evidence supports.

The second large point I would like to make is that the proposed amendments would add complexity to the guidelines. As the Commission recognizes, the guidelines are not intended to capture every possible permutation imaginable and only when the data permits should it conclude that a factor is not accurately accounted for. We are not aware of any data that would support these amendments. The Commission has announced a long-term goal of simplifying the guidelines, and these proposed amendments stray far from that path.

Turning now to a few of the
specific factors, because I won't be able to address them all, is, first, I would like to address the treatment of victims in Section 2(b)1.1 and the question whether individuals whose privacy has been violated or who suffer some other non-monetary harm that cannot be measured in terms of money should be treated as victims or otherwise accounted for under that guideline because, if they are so treated, the guideline ranges for some, perhaps many, will increase. We oppose such a change.

Let me emphasize at the outset that we do not mean to suggest that individuals who commit computer crimes or identity theft should not be punished or that there's never a case involving circumstances that are particularly egregious in regard to non-monetary harm. Rather, we have seen no data indicating that judges frequently impose above-guideline sentences on the basis of privacy violations or in order to impose additional punishment for harms that cannot be
measured in terms of money. And it's not because courts don't have the tools to do that. Application Note 19 invites upper departure if the offense caused or risked substantial non-monetary harm, and courts can, otherwise, vary upward when appropriate. For this reason alone the Commission should not act to expand the definition of victim or create a role that would increase punishment based on a new measure expressed in terms inevitably subject to challenge and litigation and that would not advance the purpose of the directive.

We, therefore, oppose any amendment that would count as a victim or in some other way provide for increased punishment [for] any individual who experiences lost time, such as time to restore credit. Victims of crime typically spend time dealing with the crime and its harms. That's why it's a crime. That people spend time resolving problems is intrinsic to the offense. It does not aggravate it.
In fact, I can personally report to you that at the very moment that I was in the final stages of preparing my testimony for this hearing some unknown person or entity used my bank check card number and my billing address to purchase pornography on the internet. It wasn't me, it was fraud. It happened right when I was finishing this, but when I saw the charge on my checking account statement I made a few calls and got the charge canceled and a credit was issued. It took about 15 minutes, and I will not suffer any monetary loss. But should my lost time of 15 minutes really translate into increased punishment for the defendant? And what would be the measure? And how would a judge evaluate the reasonableness of the time I or any other person spent?

Part of my 15 minutes was spent interrogating my teenage son to make sure he was not the criminal. And what purpose of sentencing over and above prosecution in the existing guideline ranges served by counting
me as a victim?

The Commission has not said exactly how it might count persons who were fully reimbursed for their monetary loss but who spent time resolving problems, but I would say the rule that counts me as a victim runs the risk of effectively counting every person whose identifying information was obtained or used. This could be just a few or it could be millions. And we, as defense counsel, are obligated to challenge the veracity of these claims, potentially turning sentencing proceedings into extensive mini-trials where I would be cross-examined on my 15 minutes and maybe about the internet habits of my teenage son. Thank you.

I would also like just to take a moment to address the proposed amendment to the definition of sophisticated means in Section 2(b)1.1. I'm not [a] techie by any stretch of the imagination. In fact, I expect others speaking after me will be far better able to explain the various uses and the
prevalence of proxy computers and other types of technology. But I know enough, being a mother of that same teenage son who's in college and whose nickname at our house is "IT guy," to say that the proposed amendment to the sophisticated means enhancement under 2(b)1.1 will absolutely sweep in conduct that is not especially complex or especially intricate. The Department would have us believe that any technology or software to hide identity or location meets that test, and it is simply not true. The Commission should resist the call to view advancing technology in the execution or concealment of an offense as a necessary indicator of increased seriousness or increased culpability.

As one researcher put it in a report on identity theft submitted to the Department of Justice, the majority of offenders engaged in these types of fraud use relatively tried and true old scams simply adapted to new technologies. And, again, we're not aware of data showing that courts
are unable to apply the enhancement in the appropriate case.

But perhaps more troublesome, by adopting the proposed amendment, the Commission would create a wholesale presumption in conflict with actual evidence. It would effectively relieve the government of proving the purportedly aggravating fact in any given case and shift the burden to the defendant to prove that the enhancement should not be followed in this case because it represents unsound policy. This is a reversal of what citizens expect when a system deprives us of our individual liberty.

I will end my comments with a general observation. In the advisory sentencing scheme repeatedly and insistently described by the Supreme Court, a change to a guideline that has [been] influenced or directed by Congress without an independent policy reason that is based on the Commission's own institutional expertise is no longer a defensible approach to developing
sentencing policy. District courts are increasingly recognizing their power and, indeed, their obligation to reject guidelines that are not empirically based. Without empirical evidence to support the proposed amendments, courts will disregard them. Thank you very much.

ACTING CHAIR HINOJOSA: Mr. Weafer?

MR. WEAFER: Mr. Chairman, members of the Commission, thank you for inviting me here to testify on Identity Theft Enforcement and Restitution Act of 2008. Let me explain my background, my view of what I see in the internet and the cyber landscape and then talk a little bit about what happened in 2008 and the last few years.

So Symantec, as a company, provides products and solutions to all the way from home users to large enterprises to government entities. We see, we have a sensors network around the world of about 40,000 sensors in about 180 countries. So it
gives us a good view of the cyber threat landscape and how it's evolved throughout the many years. My own personal experience is about 15 years watching the evolution of the cyber threats from the old teenage hackers all the way to the open-source communities' evolution to the very sophisticated criminal organizations that we see today running many of these scams.

So in terms of cyber crime and how we view it, we have a very broad definition ourselves. We look at it and say that it's defined as any act which are committed using a computer software or hardware. Now, we look at two different types. We look at class one, which is really a single act, typically a virus infection, a fishing attack or removal, so the actual act typically is done in one stage. Of course, the remediation, recovery of your identity, could take hours, minutes, years in some cases. And the second is type two, which is really things like stalking, blackmailing, continuous aggravators, types of
actions upon the victim or person.

We look at the cyber threat landscape, we published in a report looking at the evolution over the last couple of years, certainly starting about the late 90s onwards. And some of the things we've seen will look as if the volume and sophistication of threats we see out there has significantly increased even over the last 12 months. Sixty percent of all viruses came out in the last 12 months alone. So if you look and think of an escalation chart, the vast majority of what we see today actually has come up in the most recent past.

Now, why is that? There's multiple reasons: the modularity of the code; the open-source communities; the cheapness; the availability; the communities, the web forums, the online IRC channels which are allowing people to get together, pick up these tools and use them. And, of course, there's the botnets which are frequently used as the engines to deliver it around to end users.

We also see that while the
majority of fishing or fraud attacks are targeted towards financial information, increasingly we're also seeing that social networking sites are being targeted because they're trusted communities. They're trusted communities towards business professionals or for teenagers or groups because attackers like to be able to segment their market, much like any business, and they like to know who they're going after.

We also see the rise in botnets. In fact, we can see, roughly, about [a] one-third rise in botnet activity in 2008. And, again, the botnets are kind of the engine we constantly talk about. It generates a spam, the fishing, the solicitations that the user gets, which they can click on or go to web sites, which, in turn, downloads to malware, which, in turn, drives them towards other crimes. So, again, these are areas where we see a rapid increase in both volume, as well as sophistication.

Last year, we did a report. We
looked at the underground economy. We decided
to look and see who's out there, what type of
services, what were they advertising, where
they are located, and what type of communities
are there. And as we went in there, we
noticed that -- and this was done in a report,
which is about a one-year period between July
2007 and end of June 2008, so a 12-month
period. And we went out and we started
looking at communities: what were they
advertising, who were the top advertisers, how
much were they trying to make, what was the
lowest and highest range in terms of
advertised goods. And we found during that
time, this was only a snapshot of what was out
there because, again, we're not seeing
everything, the total value of the advertised
goods and services was about $276 million.

Now, it ranges, of course. Not
every goods and service is going to be bought
and sold. Not everything, of course, will be
trustworthy. If you actually delivered all
those identities and all those credit cards
and all those bank accounts, the total value is closer to $6 to $7 billion of what we were looking at.

What we did find is that, even though it was kind of an open source, there were very organized groups. There was strong evidence of organized crime and other entities being involved in terms of organizing these groups. There are definitely individuals who are involved, loosely-linked individuals coming in. And they're playing portions of this cybercrime landscape or life cycle either because they're getting involved in mules or money laundering or creation of tools and services. So there's a whole group of people who have been kind of brought into this area, but some are very organized and very targeted of what they're looking for from all the way to the very top end, which are targeting towards governments or industries with these so-called zero-day attacks, which are unpatch attacks.

We also looked at who were the top
advertisers. In other words, were these just randomly distributed across multiple people? And we found that, in general, the top advertisers constituted the bulk of what we saw in terms of value and the amount of volume of advertising that was going on there.

So these people generated top advertisers about 70,000 distinct messages and advertisements with about 44 million messages going out. So think of messages being relay chat channels, e-mail channels advertising their business. So 44 million times they went out there and about 70,000 advertisements. And the total value of those goods was about $80 million for those top ten alone.

So it gives you an idea of how it's consolidated into relatively small groups of people first. And, of course, the types of goods and services run the gauntlet from, of course, bank accounts, credit card information, but also tools, services, as well as things you wouldn't normally think of, such as travel services, other things which could
be bartered and traded for knowledge or money.

Now, we believe that we've arrived at an inflection point where the amount of bad code or malicious code actually is out producing the amount of good code that we see on a daily basis. So when we look at users' machines, we find that the vast majority of new code coming on to unprotected systems is actually malware, malicious code. So we do need to make sure we're very clear in terms of our laws and our sentencing towards this.

What we find, certainly on a global basis, is that, today, we still find too many countries where their definition of cybercrime, where the laws associated with cybercrime are ambiguous or non-existent, and that's certainly a problem. Certainly, where we see many, many of these players acting around the world, consistency in laws and having a model so that other countries can look at is very important.

It's also important that we can have laws which distinguish around behaviors
and intent, rather than technologies. And we
do agree with this, which is technologies can
be used for good and bad. Certainly, some of
the technologies mentioned here are used in
common applications, so you've got to be very
careful what you're looking at, what the
behaviors and intent as you're looking at how
serious is the crime.

We definitely want to make sure
that we're still not relying on terrestrial
laws or ones which don't take into account the
virtuality of the internet and the ages coming
with this. We do think we count these with
limited deterrence, and, certainly, we're
seeing too many users which are being just
onslaught with new attacks coming on a daily
basis. So we do need to send out a strong
message there.

Self protection still remains the
first and last line of defense for most
people. Go out and put on credit monitoring,
go out and put on security software. So in
reality, they're not feeling they're getting
a lot of support out there.

We do believe that a global model is very important for us and that we need to make sure that what we do here can be lifted into other countries or used as models, so they can also get the benefit from this learning. Thank you.

ACTING CHAIR HINOJOSA: Thank you, sir. Mr. Schoen?

MR. SCHOEN: I'm still waiting for my microphone.

MR. WEAFER: Keep the red button up.

MR. SCHOEN: Thank you. Chairman Hinojosa and members of the Commission, thank you for the opportunity to testify today on behalf of the Electronic Frontier Foundation. I'm here, in particular, to testify about the matter of the treatment of proxy servers and similar technologies as sophisticated means by the sentencing guidelines.

At the Electronic Frontier Foundation, my title is Staff Technologist,
and I've held this position for seven years. I'm a computer programmer and not a lawyer, and I do research on civil liberties implications of technologies, and I try to educate the public about the intersection of technology and individual rights.

So this year the Commission has been looking at computer proxies and similar technology, as several previous witnesses have mentioned. And we now have specific language. The Commission has proposed this text, "In a scheme involving computers, using any technology or software to conceal the identity or geographic location of the perpetrator ordinarily indicates sophisticated means."

As I'll explain, EFF opposes this amendment. In particular, we oppose this amendment because we think that it's over-broad and that it will sweep in a wide variety of ordinary and non-sophisticated conduct and technology.

These technologies that may have the effect of concealing the identity or
geographic location of an individual are actually used routinely by a wide range of people for a wide variety of purposes, most, though not all of which, are unconnected to criminality or criminal activity.

Technologies like computer proxies may have the effect of concealing someone's identity or location, but they don't necessarily require technical sophistication on the part of the user or indicate any unusual expertise. They don't necessarily contribute to avoiding detection, and they don't necessarily indicate pre-meditation or a commitment to a course of criminal conduct, which might all be possible rationales for imposing additional incarceration for this behavior. Therefore, there's no reason to consider the use of proxies and similar technologies to be sophisticated as a general rule or to create a general presumption that the use of this technology is a sophisticated activity. We do agree that the use of proxies and similar technology might sometimes
indicate sophisticated means, but we think this is a case-by-case determination that can best be made by a court.

So let me just talk briefly about what a proxy is. And then I'll talk briefly about a few reasons that people may use proxies and who some of the people are who are using proxies.

So we can make finer-grained technical distinctions. And last year I was a co-author of a book called "How to Bypass Internet Censorship," which talks about one application of computer proxies, particularly in countries that have technical censorship of the internet where the government actually blocks certain materials and actually prevents people from going to certain sites. And in that book, we made finer-grained distinctions based on the technology underlying proxies. I think for our purposes today those distinctions are not necessary. We can say simply that proxies are computers or software that act on behalf of someone else, on behalf
of another computer, or on behalf of another program, and they carry out a request.

So instead of communicating directly, one computer can communicate via a proxy. It sends a request to the proxy and says, "Please do the following thing for me." If the proxy has been configured to comply and the user is authorized to use that proxy, then the proxy will make the request on behalf of the original user, on behalf of the original computer, and then send back the results.

We made the comparison to the children's game of telephone where children in a line whisper something to each other and then whisper a response back. Computers are a little bit more precise and a little bit more accurate than school children that way, but the structure is similar. One person is passing on a message, one computer is passing on a message for someone else.

And the most common example of this would be for web browsing where we have proxies that download web pages on behalf of
someone who is using the web. One consequence of this is that the end user's computer and the web server that hosts the web page that they're interested in do not communicate directly because the entire communication is mediated by that proxy. So the other party to the communication sees the request, sees the activity as though it came from the proxy, rather than from the original user's computer. At the very least, this would create an extra step in identifying the identity or location of the user. Now, the proxy may or may not have been designed to have that effect, but, typically, it would have that effect because it is another computer that's in the path, another computer that's part of that process. And the reasons that people might use these technologies could be very various.

We've dealt with proxies quite a bit. As I mentioned, I was a co-author of a book about bypassing internet censorship. In countries like Iran and Saudi Arabia and China where governments use technical means to
control access to certain information, people often use proxies to circumvent these restrictions. And that's one application, and that's an application that we discuss quite a bit, and we discussed several technologies that can be used for that purpose.

We also previously funded the development of a project called Tor which is probably the most popular public proxy network in the world. It's a privacy-enhancing technology. I'm happy that the leader of the Tor project, Roger Dingledine, is attending this hearing today, and he said that he would be happy to talk to any members of the Commission or any staff who might like to discuss that technology with him. And we're still advising the Tor project on their independent organization.

So I'd like to briefly look at this question of whether proxies are appropriately described as sophisticated and whether the use of technology of this sort is appropriately described as a sophisticated
means under the sentencing guideline. So I think the most important point to make in this connection is that a user doesn't have to be sophisticated in order to make use of a sophisticated technology. In our modern society, people use all sorts of things that were a substantial engineering effort to create like a car or like Microsoft Word, which took engineers years and years of effort to create, but they're often used by teenagers. They're used, essentially, by everyone in our modern society.

So we have this kind of one level of disconnection between what was the engineering work that went into making an artifact and then what's the special skill, what's the level of knowledge that the people who are using it have. And I think it's clear on reflection that people who are using proxies generally are not very sophisticated. This is an everyday technology. This is a mainstream technology. This is a technology that large numbers of people use without even
being aware of it, without even knowing that they're using a proxy in many cases. And I have a few examples of that in my prepared statement, and I'll try to get to a few of them today.

Furthermore, proxies in general, as far as technology goes, are not particularly sophisticated. The concept of a proxy, a computer that acts on behalf of another computer, has been around for many years, has been implemented many, many times independently in a short time.

While I was preparing this testimony, I decided to write a proxy myself from scratch, and it took me five minutes and 15 lines of computer code, which is pretty short as computer programs go. And it worked, and I was able to browse the web through it. I could have one computer over here sending requests to my little proxy program, which then repeated the request to the web server that I was interested in accessing, and that worked fine. So even from the engineering
effort point of view, the proxy technologies are not necessarily particularly complex.

There is kind of a continuum. The Tor software that I mentioned earlier is quite sophisticated. It was originally funded by the Naval Research Laboratory. It involves really Ph.D.-level research. But on the other hand, some proxies are something that someone could create in a few minutes just based on the basic concept.

Nonetheless, Tor actually has over 100,000 regular users and a lot of evidence, although most of it is necessarily anecdotal, suggests that most of those users are not sophisticated computer users. They're not experts. They went to the Tor web site, they followed some very simple steps that were very straightforward, and then, like a car driver, like someone writing a brief in Microsoft Word, they were able to get the benefit of this quite sophisticated technology without having the expertise of their own. So Tor is sophisticated technology, but its users
generally are not sophisticated users.

So in the interest of time, I'd just like to give three examples of reasons that people may use proxies routinely that don't necessarily reflect criminality or criminal intent and where often the users may not be aware that they're using proxies or, in any case, have some entirely non-criminal purpose for having done so. And in my prepared statement, I have several other examples.

One example is a corporate virtual private network. So a lot of businesses set up this technology called the VPN that will allow someone who works for that corporation to get remote access to the corporate network when they're traveling or when they're at home working from home instead of in the office. And this is a secure encrypted technology that produces the effect of making it as though the end user's computer were inside the corporate network, even though it's really somewhere else. And then the user can get access to
corporate resources. Often, they can actually browse the internet and do other things through that virtual private network. And, again, the virtual private network acts much like a proxy there. The communications are all mediated through, routed through, transmitted through that corporate network.

A lot of people have been issued laptops by their employers that have this technology already set up. They might not even be aware of it. If they are aware of it, it's typically one button that they have to click and then, thanks to their corporate IT department, all of their communications are going through their employer's network. And I think that the use of that technology would be covered by the proposed amendment text as written because, certainly, someone looking at those communications would say, "Oh, they came from this corporation," whereas, in fact, the user who is ultimately responsible for them was physically located somewhere else.

Another example is a library
proxy. So a lot of research libraries have subscriptions to journals or services like LexisNexis and commercial databases that are limited to use by subscribers and by subscribing institutions. Often, this limitation is enforced by looking at which computer network someone is coming from. So the operator of LexisNexis or a journal would say under this subscription this can only be accessed from on campus. And so the library then has the problem what if people want to use it from off campus? And a very large number of research universities have set up proxies that can be used by any student at the university, and it does conceal the location or the identity of the user. It makes it look as though they're on campus temporarily so that they can use those resources that are limited to subscription purposes.

Interestingly, I think that can be so easy to set up that you could do it once and then you could forget about it and you could keep on using it. It's a very simple
thing. And not only the computer science majors use it, but also liberal arts and humanities majors will use this to get access to these academic resources from off campus.

And the final example would be the use of proxies or virtual private networks to protect individuals' privacy when they're accessing the internet from, for example, public networks that they don't trust. So one example would be using a Wi-Fi network in a café to access the internet from a laptop.

Now, an interesting fact about Wi-Fi networks is that every other user on the same Wi-Fi network can see all of the communications that a person transmits. And there's very simple, well, I don't know whether I want to say whether that's sophisticated means, but there is straightforward, publically-available, freely-available technology that would let people spy on all of the communications of other Wi-Fi users. And I've had this concern when I've been in cafes or at conferences: is somebody
sitting here with a laptop spying on my communications? And a very common and an increasingly common response to this is to use virtual private networks and proxies. Symantec is actually a well-known developer of the virtual private networks that people may use for this purpose so that their communications are protected and can't be intercepted by the other people on that network. And so that's actually a use of proxies and VPNs and the like that people make to protect their privacy and protect themselves against things like identity theft. People will also use technology like Tor in that situation.

And so, again, this is something that they might set up once, and then they say, "Okay, now I'm protected," and they continue to use it on an ongoing basis. So it's not necessarily a matter of getting up in the morning and saying, "I'm going to figure out how to use a proxy today." It could be put into the computer's default settings and
then take effect every time the person uses
the internet.

I think in the interest of time,
I'm going to stop there. I would refer the
Commission to my written statement which has
several other examples of reasons and
situations and purposes where people might use
proxies. I think the overall message is
proxies are a basic and widespread and
increasingly widespread part of our internet
infrastructure. They're used by a lot of
people for a lot of purposes everyday. They
can have applications that are criminal
applications. Criminals can use them.
Criminals can benefit from them. But the
majority of uses and the most typical uses are
non-criminal uses that are routine uses by
unsophisticated people.

So for those reasons, EFF opposes
a presumption that the use of technologies of
this sort would be considered sophisticated
means. Thank you very much.

ACTING CHAIR HINOJOSA: Thank you,
Mr. Schoen. And I'll guess I'll start off with the first question. Ms. Coffin, on behalf of every person here who has ever dealt with their credit card company or the power company or the cable company, we congratulate you on being able to get such quick results, I have to say. Did you cancel the card or what did --

MS. COFFIN: I did. It was a phone call.

ACTING CHAIR HINOJOSA: It was one phone call? You canceled the card. They canceled the -- they didn't give you the 30-day that everybody else gets or anything else? I think we all should hire you. Obviously, if it was 15 minutes, a sentencing court is going to, if there is an allotment with regards to your time, figure out what 15 minutes of your time was as opposed to had it been over a 30-day period or a 60-day period that you were left in limbo with regards to your credit card. And I assume that you had not used your credit card to be in place with regards to any
other payment where you had to call them and
cancel all the payments, as some of us do with
regards to automatic payment. And I assume
that was not affected by this card. So you
were lucky, and so my question is, let's say
it had been somebody else who didn't get the
luck of actually finding somebody within 15
minutes and [being] able to get [the card]
canceled immediately and the charges taken off
without going through the regular procedure.
It would not change your mind if somehow
somebody else was put through a lot more than
you were and that particular victim should be
treated exactly the same as you would be if it
only took you 15 minutes?

MS. COFFIN: It's not that my mind
needs to be changed. It's that I think that
the guideline already adequately accounts for
those unusual circumstances. In the written
testimony, I suggested that perhaps there
might be circumstances, the unusual
circumstances, if you go by the Federal Trade
Commission's report, that some ten percent of
the 8 million people who have reported that
their identifying information has been
misused, that that would be an unusual group
of people and that if we do anything it should
be to sort of recognize that it's in the
egregious cases that a court might want to do
something different with the recommending
guideline --

ACTING CHAIR HINOJOSA: So I take
it you would not object to a departure
application note or something that would take
care of those cases or possibly an SOC that
would be applied in a smaller number of cases?

MS. COFFIN: If I had to choose, I
would choose the departure application,
obviously, because what happens I think is,
obviously, we're concerned with the adding
complexity to the guidelines when it's not
necessary because I think a judge, in a
situation where they're faced with someone, an
identifiable person who can come in and say
this completely upended my life and I was on
hold for many years, that's something a judge
can take into account already. I'm not sure that we even really need to do everything to the guideline, but if you had to do something we would prefer a departure provision.

ACTING CHAIR HINOJOSA: Who's got -- Ms. Howell, let's start with you.

COMMISSIONER HOWELL: I have two questions; and since the Chair started with Ms. Coffin, I'll ask you this one, as well. One of the things that you said quite strongly and articulately is that in Section 209(a) of the directive in the ID theft law, [] we were supposed to focus on the 13 factors to create an effective deterrent. But another part of this directive specifically states that we are supposed to reflect the intent of Congress that such penalties be increased in comparison to those currently provided by such guidelines.

Now, it's taken from your comment that we're supposed to ignore the specific directive to increase the penalties compared to those currently provided by the guidelines.
if we can't find empirical research to support it. Is that the import of what you're saying is that we should only look at empirical data and forget the congressional explicit directive to increase the penalties?

MS. COFFIN: Well, actually, what I'm saying is that I understand that Congress is sending the Commission somewhat mixed signals in this directive. On the one hand, you have a general inchoate statement from Congress about its intent: that penalties should be increased. On the other hand, you have Congress giving you very specific direction to study and do research on factors, eight of which, by the way, the Congress has already directed the Commission to examine and it did. But what Congress is saying is, ultimately, sending the message that the Commission is being expected to act as the independent body that does research.

And I also understand, of course, that the Commission feels pressure to respond to every little directive, and you've got two
here that kind of go both ways. And so the
Commission sort of has a choice. What does it
do when it has these two forces coming at
them? And the question, of course, that has
to be asked and the judges will ask is: is the
guideline a reflection of your institutional
knowledge or is it just a reflection of a
congressional directive.

And of course, this is not a new
tension. This is something that the
Commission has been dealing with for a long
time. And I, personally, have done some
research on all of the directives, and I
understand that the Commission has in the past
not acted on directives and that's something
that can happen. And it can actually report
back to Congress and say, "We looked and we
did what you said and we decided that, in
order to actually satisfy your directive,
doing the job that we have been charged by you
to do, we cannot say that increasing penalties
will create an effective deterrent, and so
that's not what we're going to do."
COMMISSIONER HOWELL: Usually, in those circumstances, it's where the directive has said review and, if appropriate, amend the guidelines. And that's usually where we look and we decide whether or not it's appropriate, and we respond accordingly. That's a different kind of directive than one that specifically directs an increase in comparison to those currently provided by such guidelines. And it's for us to look at all those different factors and decide which ones we think, based on the factors and evaluation of the empirical data, deserve an increase.

But this is a position of the Federal Defender that goes far broader than just this law and just this directive. And I just wanted to be clear that it sounded as if you were saying look only at the empirical data and not at the specific explicit statutory requirement that the Commission has been given to increase some of the penalties compared to current guidelines.

I want to turn for a second to Mr.
Schoen's comments about proxy servers. I have to say, after reading the Department of Justice's testimony and EFF's testimony on proxy servers, I had to go back to our original proposal and look at it more closely because I hear from the Department of Justice that it supports our enhancement on the sophisticated means enhancement, in part, because it will provide more consistency across the country in terms of use of proxy servers in connection with different computer crimes. I hear from EFF you think that it's also, EFF prefers a case-by-case approach.

What our proposal essentially says is that, you know, in a scheme involving computers using any technology or software to conceal the identity or geographic location of the perpetrator, it ordinarily indicates sophisticated means. So it's actually not a directive to the court that they must apply this enhancement or consider it sophisticated means if there are proxy servers used. And so I was interested to hear whether -- so I sort
of view this "ordinarily indicates" as not a directive to the court but, in fact, you know, a requirement that they're going to have to look to see on a case-by-case basis whether or not an effort to conceal the identity or geographic location either through proxy servers or some other means is an indication of sophisticated means.

So from DOJ's perspective, do you think that this language is a specific directive to the court that [the] use of any proxy server is one example of hiding identity or location [and] is going to necessarily trigger a sophisticated means enhancement, or do you think it's still going to require a case-by-case analysis of the actual means used to commit the offense?

MR. DUBOSE: I think it would still require a case-by-case analysis. Obviously, ordinarily, I think the use of the term "ordinarily" gives strong guidance to the courts. And I'd also kind of reiterate because, actually, I agreed with very much of
what the Electronic Frontier Foundation said because we agree that, you know, just use of proxy servers in and of itself is not illegal.

COMMISSIONER HOWELL: As do I. I agree with that, as well.

MR. DUBOSE: But in the context of this guideline, the way it's written is when you're using that server, after having been convicted of a crime and it's being used as part of a scheme in that crime to hide your identity from law enforcement, that is when, in our view, it's not that it is, in and of itself, a technologically sophisticated software. It may or may not be, depending on who designed it or whatnot. It's not even that the user of that software is necessarily technologically-sophisticated but, rather, that the use of that software in the context of the scheme or to the fraud that's using the computer is the type of action or behavior that's intended to be covered by the guideline itself, which right now 2(b)1.1 (b)9 says if the defendant relocated or participated in
relocating a fraudulent scheme to another jurisdiction to evade law enforcement or regulatory officials or a substantial part of a fraudulent scheme was committed from outside the U.S. or the offense otherwise involves sophisticated means increase by two levels.

What we would assert is that, first, as Mr. Weafer I think testified that, you know, what we also have seen where there are a lot of countries where the computer crime laws [are] inadequate or they are non-existent, and those very often are the jurisdictions where criminals are using proxy servers so that they'll bounce, when I first encountered this eight years ago trying cases, we referred to them as bounce servers or bounce boxes, not proxy servers, but same function different name which is if they would route their electronic communications to a box in Russia it would then be transmitted back to maybe, you know, a target computer in the U.S. When you are investigating as law enforcement, it looks like it's coming back to Russia and,
you know, our law enforcement relations with Russia are improving but they're not that good. And for the most part, that's a black hole for us when it comes to getting law enforcement cooperation.

And so, you know, from a law enforcement perspective, that's the equivalent of placing your telecommunication fraud company in another country, if not more so, because it not only makes it difficult, it makes it virtually impossible to gain attribution in that crime. And that's what we think really falls within the intent of this guideline as sophisticated means.

COMMISSIONER CARR: Let me ask something. Mr. Schoen, part of the tone of your comments almost made it sound like you were concerned that we were criminalizing the use of proxies on their own, when, in fact, you already have to be involved in a crime and then the question is whether or not the use of a proxy to conceal the identity or location of the person committing a crime would trigger
the presumption I think would be fair in terms of the language of the proposal here.

Are you troubled if someone who is committing a crime is using a proxy for the purpose of avoiding detection of the person or the person's location? In other words, it has to be both. The proxy is being used, and you were giving examples where someone might forget they're using a proxy or might not know that they're using a proxy. But if the purpose is to conceal the defendant or the defendant's location, does it trouble you less that that would have a presumption of being a sophisticated means?

MR. SCHOEN: Well, I'm not sure from the proposed text whether it's meant to require a purpose or intent rule. It says the use of technology to conceal, and I don't know whether that's meant to be read as with the intent to conceal or with the effect of concealing.

COMMISSIONER CARR: Okay. I assume that the first would trouble you less
than the second?

MR. SCHOEN: Yes, I think that's correct. If we're looking at it under the lens of sophistication, I'm still troubled by that lens in this case, simply given what I know about proxies and my experience with them, just thinking in terms of the sophistication of a person or the complexity of the acts that they have to do because, as my written testimony explains, I think that the acts that people have to do are not particularly necessarily complex.

COMMISSIONER CARR: Okay. But given the kinds of things we've sometimes used as enhancements, just like using offshore bank accounts, they don't necessarily have to be unbelievably sophisticated or unbelievably inconvenient in order to trigger an enhancement.

MR. SCHOEN: So I think that, within that context, the reason that I gave several of these examples was to point out that someone might have their identity or
location concealed by technology without having a criminal intent to do so.

COMMISSIONER CARR: We've already got a criminal intent if we're looking at this enhancement. Then the question is whether there's an added intention to conceal them.

MR. SCHOEN: Yes.

COMMISSIONER CARR: You need the underlying crime, for starters.

MR. SCHOEN: Yes. I'm just saying someone might have a computer, like a computer issued by their work, that because of the way it's set up with the virtual private network they don't know --

COMMISSIONER CARR: Understood, understood.

MR. SCHOEN: And then they may commit a crime and have an intent to commit a crime, but they didn't have the intent to hide their location, even though it had the effect of doing so.

COMMISSIONER CARR: Thank you.

Ms. Coffin, I don't know whether you're a
harsh or skeptical enough interrogator of your son that he might have been a victim here even if you weren't, so I won't get into that.

MS. COFFIN: I was going to ask what was Seth's computer proxy doing while I was working on this.

COMMISSIONER CARR: As Commission Howell said, you make an eloquent presentation with respect to deterrence and what the literature is out there in terms of what does and doesn't deter. Even though most people would assume there's a logic to harsh penalties deterring conduct, I realize that the literature may question or contradict that.

But you do mention that certainty of punishment is known to deter. We have somewhat of a broad charter from Congress; it might not be quite this broad. But should we be paying any attention to ways in which certainty of punishment could be enhanced in this country, as opposed to just the level of punishment?
MS. COFFIN: I often wonder if part of the Commission's charge is to think about issues a little bit more broadly than just how do we amend the guideline [this] very amendment cycle, and I know that you do that.

COMMISSIONER CARR: And it absolutely is.

MS. COFFIN: And it also occurs to me that perhaps the Commission could do a broad study of all of the literature and maybe all of the issues related to identity theft because there's a lot out there, and I know because I had to travel through a lot of it when I was thinking about this. It seems to me like the Commission could, as part of its approach to these kinds of issues, to put together something for Congress or for law enforcement to sort of explain that the solution may not lie always in increasing punishment and to maybe explain what other ways, what other prevention mechanisms might go into place. And that could be something that could involve lots of different entities...
and how they go about doing it. And that, I believe, is something that the Commission could do and should do and would be a great piece of information for how we go forward and how we do this, yes.

COMMISSIONER WROBLEWSKI: Thank you, Judge Hinojosa. First let me thank everybody who's on the panel. We really appreciate you all being here and participating, and I think the discussion has been very, very productive.

I've got one question for Ms. Coffin and a question for Mr. DuBose and Mr. Handy. Ms. Coffin, you've talked about the need and the Supreme Court talked about the need for empirical research, empirical information to be the basis of the guideline amendments and the guidelines generally. Do you consider Mr. Schoen's testimony to be empirical information?

MS. COFFIN: I consider his testimony as supporting evidence, and I guess you could put it as empirical information, to
a certain degree, to support I think the very simple proposition that the use of a proxy or the use of technology like a proxy, even if it is to conceal your identity or conceal your geographic location, that that doesn't always meet the test of the sophisticated means enhancement. In other words, we kind of skip over that part when we talk about it when we say, "Well, if we're doing it to conceal identity, then isn't that worse?" But the Commission has already created enhancement that says that to satisfy the test it has to be especially complex or especially intricate conduct. And in my experience, courts often skip over that, too, and they go straight to the examples and they forget to ask whether the conduct actually meets that test.

So our concern, of course, is that by putting the language in there the way it is, and it will work in practice, like presumption, unless you have someone who's really ready to completely fight it and a judge that's willing to listen. So that, yes,
I think what you've gotten is, to a certain degree, you've gotten some empirical evidence that supports the conclusion that the proposed language would sweep too broadly.

COMMISSIONER WROBLEWSKI: How about Mr. Weafer's testimony? Is that empirical information?

MS. COFFIN: About the prevalence of cybercrime and the way that it's happening?

COMMISSIONER WROBLEWSKI: The changing landscape over the number of years, the number of attacks that have happened in this year, the number of viruses this year being more than any other time?

MS. COFFIN: I do think that's the kind of evidence that the Commission could use to put together or compile the kind of information that Commissioner Carr was talking about where we're saying okay, yes, things have changed. Is the solution to increase penalties? No.

COMMISSIONER WROBLEWSKI: And --

ACTING CHAIR HINOJOSA: Can I just
interrupt you for a second? Because I think it is important when one of the statements made to us is that we shouldn't just pay attention to directives. And I guess my question is in the Sentencing Reform Act that includes the enabling provisions for the Commission, where is the portion that says that the Commission is to rely solely on empirical evidence and on nothing else, and what do we mean by empirical evidence? I guess that's the question that's coming from some of us here. Where in the statute itself does it say you are no longer to pay attention to us in the future, even though we passed the laws and including the Sentencing Reform Act, and you are to base decisions based strictly on empirical evidence and on nothing else and that that becomes the overall role of the Commission with regards to what we do? Because what part of the statute says that over anything else that we hear from either Mr. Weafer or Mr. Schoen or the judges or the defenders or the prosecutors or victims or
anybody else who sends us comments and we go
through this cycle that is a long nine-month
to a year period to make decisions as to how
we fit into the 3553 factors? I guess that's
my question.

MS. COFFIN: I think I quoted to
you the part that I believe best captures the
idea that what the Commission's original core
organic purpose is to do which is to develop
sentencing policy that reflects the state of
human knowledge and human development as it
relates to the criminal justice system. And
it is true, and I'm not suggesting that the
Commission is not supposed to listen to
Congress or the Commission is not sometimes
under direct orders to take particular acts.

But in this particular case, I
think that the language of the directive is
not so mandatory that the Commission must act.
And so in that case, the question becomes what
in this new landscape that we have I think,
after the Supreme Court has just finished with
these five cases, the question for the
Commission now is really an opportunity to do what the Commission probably has really wanted to do for quite some time, and it's felt always under pressure to respond to congressional directives. And I would suggest that right now the Commission has an opportunity and a directive on its table that it can use to implement its institutional expertise.

And I think, too, that that's really what judges are looking for. Judges are looking for guidance that will guide them that they can say, yes, this comes from the Commission who has done [a] study and has looked at this and has taken testimony from people and listened to everything and decided that this is the correct course of action and not look at a guideline and say, well, Congress told them they expected sentences to go up, and so they did. I think that it's a tension, and I think, though, that that's the ultimate choice that the Commission should make.
ACTING CHAIR HINOJOSA: Well, it's a tension that you face in the courtroom, tension that you face in the Sentencing Commission, tension that Congress faces. It's a tension with regards to the whole putting it all together, but I think that this is something that the Commission for years has been doing, which is looking at the 3553 factors. And we do it differently than I do as a judge in the courtroom who sentences seven to eight-hundred people a year. I mean, I have the sentencing hearing, and I look at it as closely as I can, but it doesn't go over the year period of what the Commission is doing. And so what I take what the Commission does in the courtroom is this is something that went on over a period of years sometimes, and they have used data, they have heard from other people also, and then these are the guidelines. And then, of course, I have to decide what to do on an individual basis. And I think that's the scheme that the Supreme Court has set here.
But it just gets back to the point, and I appreciate the fact that you've indicated that, yes, we should read the directives and decide how mandatory they might be or otherwise and that we should certainly not ignore them and go ahead and visit and look at them. And so I appreciate that.

MS. COFFIN: Well, if I could just add one more thing. When you asked what kinds of information the Commission should be looking at, another very important piece of information, also something that the Commission uses all the time, is the feedback from judges. They look at the departure rates. They look at the rate at which courts are feeling like a particular guideline is not adequate. And I'm suggesting that, perhaps in this circumstance and in all these amendments, there is no indication that judges are feeling like the guideline ranges currently in place are inadequate. And that is feedback that the Commission looks to and has historically looked to as one of the pieces of data that it
uses to decide whether to change a particular sentencing policy.

    ACTING CHAIR HINOJOSA: Does anybody on my left have any questions? This is the quiet side. Commissioner Reilly, we congratulate you on the green.

    COMMISSIONER REILLY: Thank you very much.

    ACTING CHAIR HINOJOSA: I interrupted you.

    COMMISSIONER WROBLEWSKI: I had one more for Mr. Handy and Mr. DuBose. Is there any -- and this will be quick. Is there any empirical information about the cost to victims? Ms. Coffin indicated her personal experience. Has there been any research about the cost to victims or the cost to people whose information is stolen and there's no monetary loss but there's time expended to fix, whether it's get a new credit card, fix credit, anything like that?

    MR. HANDY: Well, I'll start with this answer. There's definitely some studies.
The Identity Theft Resource Center has done quite a few studies. Every year we do a study on that very fact because we have the victims that call in. We have about a thousand or so victims that will call in per year or so, and we do a survey to find out what happened, how they'd go through it, what stage are they in, how long it takes those folks to complete.

Now, there are some statistics. Unfortunately, I didn't memorize them or bring them here today because I know we're talking more business than victims, but there are definitely some statistics. I'll try and remember off the top of my head what the latest, but it is very time-consuming when this happens. Now, this is great for her. Fifteen minutes is excellent obviously, but I can tell you a hundred other stories where it took months, years. Again, Nicole, who was scheduled to speak here today, eight to ten years still fighting. So that's more like what I'm hearing. The 15 minutes is not the norm for me, but I'm hearing months to correct
some of these things.

Now, if you catch it early it doesn't take long to fix it, and that's why prevention is such a key. And if you catch it early, like in this case here, it's not that bad. The problem is people aren't checking their credit reports, aren't doing the things that they need to to protect themselves, and then they find out eight months later that they've been hit, and that's where the problem starts because you have the thief going around opening all kinds of accounts and creating problems, and you're caught here and you're trying to catch up, but they're still going. And that's when you get the problem where it takes eight to ten years to solve the problem.

ACTING CHAIR HINOJOSA: On behalf of the Commission, thank you all.

COMMISSIONER CARR: To Mr. DuBose -- I'm sorry. I think the ex officio from your office asked you a question.

MR. DUBOSE: It wasn't a setup, I promise. I agree with what Mr. Handy just
said. Let me just say, you know, I don't want to concede this point of deterrence first. Our experience prosecuting these crimes is that, actually, where we're seeing this kind of massive commercialization of cybercrime, particularly with respect to ID theft and data breaches, it's very important that it not, that the signal not go out to this community that it's just a cost of doing business because the business is really thriving, and so small costs is not going to have much of a deterrent impact.

And the other thing I would mention is that, while these are global networks, that it's actually a fairly small community online and that word of sentences travels very quickly. And this goes out, it's not through the normal press, it's through IRC chat, it's through forums and through other means. So our experience is that sentences, particularly sentences that result in real prison time, have a dramatic effect and deterrent effect on the community. It doesn't
resolve the issue. Everyone doesn't pack up
and go away, but it really does have a ripple
effect that's much more significant than we
see in some other areas of crime.

In terms of the cost to victim, if
you take, as one of our proposals was that,
while we think that, generally, in terms of
the theft of types of information that it's
better to give courts flexibility in how to
assess the cost of that, whether it's fair
market value or development costs. But in
another kind of related class of cases, which
Congress recognizing ID Theft Act, one of the
reasons that they amended 1030(a)5 to remove
the requirement that you have to prove $5,000
in damages to get a felony and instead now
it's just you have to show damage to ten or
more computers, one of the reasons they did
that was in recognition of these huge botnet
cases where you have thousands if not hundreds
of thousands of computers are infected by
malware, and it would be virtually impossible
to show all of the damage to those computers.
In those cases, what we propose is that, given that the reports are that even in a fairly simple case where you have a malware loader on your computer, what would it cost to remove that malware? There are reports that we've cited in our testimony ranging from $180 to $578 for removing that malware just as a normal cost. We've actually proposed a much more conservative figure as an alternative minimum loss amount in those cases of $50 per computer, similar to the minimum loss amount in credit card cases. Thank you.

ACTING CHAIR HINOJOSA: Thank you all very much, and we certainly thank you for your thoughts and your time. We'll go on to the next panel.

The next panel is on the William Wilberforce Trafficking Victims Protection Reauthorization Act of 2008. We also thank you for your presence here today. The first one will be Mr. Joseph Koehler who is the deputy -- did I get that correct?

MR. KOEHLER: That is correct.
ACTING CHAIR HINOJOSA: Who is the Deputy Chief of the Criminal Divisions Immigration Unit in the U.S. Attorney's Office in the District of Arizona. He has served in the criminal division since 1992 handling a variety of cases, and he obviously specializes with regards to issues on immigration law.

We also have Ms. Leslie Whitcomb Fierst, who is an Associate in the Business Litigation Group of the Northern Virginia office of Womble, Carlyle, Sandridge & Rice. Ms. Fierst previously served as an Assistant Federal Public Defender in the District of Maryland and, before that, in the Federal Defender office in Charlotte, North Carolina.

We have Ms. Karen Stauss, who is a Managing Attorney and Policy Counsel for the Polaris Project where she manages the project's legal services and policy advocacy effort. She has represented human trafficking victims in immigration-related applications, and she has also worked in [the] Human Rights Watch Field Office in the Republic of the
Congo and has worked on human rights issue in Nigeria and South Africa.

Last is Mr. Charles Song who is the West Coast Pro Bono Manager for Howley LLP where he leads that organization's pro bono efforts throughout California and Salt Lake City. Recently, he served as the Legal Services Director of the Coalition to Abolish Slavery and Trafficking and previously served as a Human Rights Fellow and Staff Attorney at the Center for Human Rights and Constitutional Law.

We welcome each one of you, and we'll start with Mr. Koehler. And the rules are the same: seven minutes. This means two minutes left, and that means it's over. I'm apparently not very good about saying it's over, but we'll rely on your good conscience. Go ahead, sir.

MR. KOEHLER: Good afternoon, Mr. Chairman, distinguished members of the Commission. My name is Joseph Koehler. Again, I'm the Deputy Chief in the Criminal
Division in the U.S. Attorney's Office in Phoenix, Arizona. I appreciate the opportunity to appear before the Sentencing Commission on behalf of the Department of Justice to discuss the important sentencing issues related to the recently enacted Trafficking Victims Protection Reauthorization Act of 2008.

My testimony will focus on three issues: first, the directive to the Commission to review alien harboring guidelines where the harboring is in furtherance of prostitution and where the defendant is an organizer, leader, manager, or supervisor of the criminal activity; second, the guidelines applicable to the new fraud and foreign labor contracting offense; and, third, other sentencing implications of the TVPRA. The Department will also submit more detailed written comments on these issues in response to the proposed amendments and issues for comment published in January in the Federal Register.

The sentencing issues raised by
the Act are many and complex and deserve a complete review by the Commission. We think this review should include consultations with victim and advocacy groups, prosecutors, defense lawyers, and others, as well as a full analysis of recent trafficking cases and related immigration cases. Given the recency of the enactment of the Act, we believe it may be appropriate for the Commission to continue work on the sentencing issues raised by the Act and beyond the current amendment year with a goal of completing implementing guidelines in the next amendment cycle.

Alien harboring and furtherance of prostitution. Section 222 of the TVPRA directs the Commission to review the alien harboring guidelines and amend them, if appropriate, where the harboring is in furtherance of prostitution and the defendant is an organizer, leader, manager, or supervisor. The guidelines at Sections 2(g)1.1 and 2(g)1.3 take an appropriately graduated approach to prostitution-related
offenses, applying different severity levels
to different prostitution-related crimes,
including interstate transportation for
prostitution, importation of aliens for
prostitution, sex trafficking of minors, and
sex trafficking by force, fraud, or coercion,
according to the level of harm involved and
the culpability of the offender.

The most egregious offenses, such
as those involving the use of force, fraud, or
coercion or the sexual exploitation of a minor
are appropriately sentenced at higher levels.

As the degree or coercion or the vulnerability
of the victim increases, so does the
applicable offense level. For example, in
United States v. Caretto, multiple defendants
pled guilty to recruiting young, uneducated
Mexican women and girls from impoverished
backgrounds, smuggling them into the United
States and forcing them to engage in
prostitution by threatening and beating them.
The traffickers in that case also controlled
their victims by holding the victims' children
in Mexico. Three defendants were sentenced to, respectively, 50, 50, and 25 years imprisonment for multiple offenses of sex trafficking. These cases carry a base offense level of 34.

In contrast, cases involving interstate transportation for prostitution in violation of the Mann Act and importation of adults for prostitution in violation of 8 US Code Section 1328, which are not based on proof of the use of force, fraud, or coercion, carry a base offense level of 14 under Section 2(g). In these cases, the defendants often recruit women into prostitution, facilitate their travel and transportation, and profit from their prostitution activities. Although this conduct is deplorable, promoting prostitution and exploiting vulnerable women who have few economic alternatives, it does not involve the use of force, fraud, or coercion criminalized under the sex trafficking statute, nor does it involve the exploitation of minors. This conduct thus
differs from the conduct that defines human trafficking crimes.

Even further along the spectrum, in contrast to the Mann Act and Section 1328 offenses, alien harboring crimes under 8 US Code Section 1324 often involve sheltering or concealing undocumented persons in locations such as homes or businesses. Often, however, unlike defendants convicted under the Mann Act or international importation cases, alien harboring defendants are not implicated in facilitating interstate or international travel for the specific purpose of prostitution. This level of prostitution-related criminal intent and the extensiveness of the criminal conduct is, therefore, lower than in many Mann Act or Section 1328 importation cases.

While the entire spectrum of these federal commercial sex and immigration-related offenses involve serious criminal conduct that must be vigorously prosecuted and punished by substantial sentences, an appropriate
sentencing scheme should recognize distinctions between these different types of offenses regarding the degree of criminal intent and the extensiveness of the criminal conduct at issue.

The graduated approach of the current guidelines recognizes that, while all forms of commercial sexual exploitation are reprehensible and warrant significant sentences, the more vulnerable the victims and the more brutal the forms of physical and psychological coercion, the more elevated the offense level should be. The congressional directive asks the Commission to reconsider the alien harboring guideline, Section 201.1, for offenses where the harboring is in furtherance of prostitution and the defendant is an organizer, leader, manager, or supervisor. Alien harboring offense levels begin at level 12, only two levels below the level 14 applicable to some commercial sex offenses, such as interstate transportation for prostitution in violation of the Mann Act.
or importing an alien for immoral purposes.

In a sense, this limited two-level disparity placing alien harboring offense levels slightly below the Mann Act and importation offense levels further below the sex trafficking offense levels is appropriate. This is so, first, because convictions for interstate transportation and importation for prostitution involve not just knowledge but specific deliberate intent to further prostitution, while alien harboring convictions require no such proof of specific deliberate intent. Second, interstate transportation and international importation tend to involve more extensive and elaborate criminal conduct than localized acts that could constitute harboring, such as conduct on the part of a landlord taking steps to conceal undocumented tenants.

Thus, in the case of adults, the current two-level disparity between alien harboring and certain commercial sex offenses is limited in magnitude and arguably
appropriate. Nonetheless, alien harboring that furthers prostitution involves increased criminality, and so should receive additional punishment, especially when the defendant plays a role as an organizer, leader, supervisor, or manager.

And I see my time is up. I look forward to submitting additional comments during questioning. Thank you.

ACTING CHAIR HINOJOSA: Thank you, Mr. Koehler. Ms. Fierst?

MS. FIERST: Thank you. Thank you again for the opportunity to appear here on behalf of the Federal, Public and Community Defenders on the TVPRA. The questions on which the Commission has sought comment are, first, whether the guidelines need to be amended to ensure conformity between the guidelines for alien harboring and those for promoting a commercial sex act pursuant to the congressional directive; second, whether the two new offenses should be referred to existing guidelines or to new guidelines; and,
third, whether the guidelines should be amended to accommodate the changes that the Act made to existing offenses. I will focus the majority of my comments today on the first question.

Section 222(g) directs the Commission to review and, if appropriate, amend the sentencing guidelines and policy statements applicable to persons convicted of alien harboring to ensure conformity with the sentencing guidelines applicable to persons convicted of promoting a commercial sex act if, first, the harboring was committed in furtherance of prostitution; and, second, the defendant to be sentenced is an organizer, leader, manager, or supervisor of the criminal activity. We believe no changes are necessary or appropriate.

First, the guidelines already sufficiently provide direction in the case of a defendant fitting the hypothetical proposed by Congress, a defendant who is involved in alien harboring and prostitution at a
supervisor or higher level. Second, a
defendant guilty of such conduct is not being
sentenced lightly under any current guideline,
nor is he being sentenced without his
involvement in prostitution and his level of
involvement being taken into consideration by
the existing guidelines and the sentencing
courts. Finally, the Commission does not
presently have reliable empirical data on
which to base any amendment. So we,
therefore, recommend that the Commission make
no changes to the guidelines in response to
the directive from Congress.

In our experience, alien harboring
and trafficking cases are infrequent and the
culpability of the defendants who are
prosecuted can vary dramatically with many
having relatively low culpability. We have
not seen any cases like that envisioned in the
directive: one, where the government has to
rely only on 8 USC Section 1324 to obtain a
conviction.

In fact, one of the reasons I'm
here today as the Federal Public and Community Defender representative is because I happened to have worked on an 8 USC 1324 and 18 USC 1591 case. In that case, my client was a Mexican national living in suburban Maryland and, after losing his job as a construction worker, he began working as a driver for Latina prostitutes. He fell in love with a young Mexican prostitute who eventually came to live with him. And, unfortunately, that young woman happened to be 16 years old. He was not a manager or an organizer of any prostitution enterprise, and he was not involved in bringing that girl or any other non-citizens to the U.S. In that case, my client was charged both with alien harboring under Section 1324 and with harboring a minor to commit a commercial sex act under Section 1591, and he pled guilty to and was sentenced based on the 1591 violation.

Across the three statutes that address alien harboring, the existing guidelines more than sufficiently address the
differing types and degrees of conduct that
the federal system seeks to punish. There are
three statutes which I've referred to sort of
informally that punish alien harboring, two in
the context of prostitution. We have 8 USC
Section 1324; 8 USC Section 1328, which
addresses alien importation for the purpose of
prostitution; and 18 USC Section 1591, alien
harboring for prostitution involving a minor
or with fraud or coercion.

The more serious sexual-in-nature
alien harboring conduct covered in Sections
1328 and 1591 call for higher statutory
maximums and mandatory minimums and are
directly referred already to 2(g)1.1 and
2(g)1.3. And so it looks to me, in thinking
a little bit more about a congressional
directive and comparing the hypothetical facts
in the congressional directive to the existing
laws and guidelines that what the
congressional directive is talking about is
not a defendant who you would be looking at
under Section 1328 where the prostitute was
imported for that purpose and not a defendant under Section 1591 where we're talking about a minor being involved or a prostitute who unwillingly or under coercion became involved. But, in fact, it seems what we're talking about is a pimp who is working with willing undocumented prostitutes, and that we do not believe is something that is appropriate for either cross-references or specific offense characteristics or any other changes to the guidelines.

Indeed, in alien harboring cases committed in furtherance of prostitution, the case law shows that the government typically charges these serious cases as violations of Section 1328 or Section 1591 or both, meaning that the vast majority of the serious cases are already being sentenced under 2(g)1.1 and 2(g)1.3. If, for some reason, there were a particularly egregious case that were to be charged only as a Section 1324 case, again which is hard to fathom since the case law shows and supports that the government
regularly charges and makes these cases as Section 1328 cases or Section 1591 cases or both, then the 2(l)1.1 specific offense characteristics would dramatically drive up the sentencing range anyway.

For instance, in a serious 1324 case under the congressional directive's description, 2(l)1.1 contains several specific offense characteristics, including for coercion or threats, the number of aliens involved, and for an aggravating role, which could result in a sentencing range as high or higher than those under 2(g)1.1 or 2(g)1.3.

So, again, if you don't have the fraud or coercion and you don't have the number of aliens to show a serious operation of which the defendant is a manager or organizer, then I really don't think this is a situation that calls for any specific offense characteristics or cross references or changes to the guideline.

Given the severe sentences that are already available under 2(l)1.1, again,
there's really no reason for the Commission to
add cross references to this type of
hypothetical violation. Cross references
specifically tend to complicate the sentencing
calculation. They encourage punishment on the
cheap by allowing the government to charge the
easiest offense to prove but then punish the
defendant for a much more significant offense.
This is not only an anathema to our sense of
justice, as the Supreme Court recognized in
Blakely, but from a practice perspective it
makes a defense attorney's job very difficult
in that we're forced to explain to our
clients, many of whom we are still building
trust relationships, senses of trust, and
going to know, often across language
barriers in these cases, why it is that
they're being charged with one offense but
will be sentenced for a much more serious
offense.

Cross references also open the
door to a lack of transparency in sentencing
because in some cases prosecutors and defense
counsel may be forced to bargain around them. They increase unwarranted sentencing disparities, as well, because in some cases they may not be applied.

I see the red light indicates that I'm up; isn't that correct? All right. Well, then I'll reserve the rest --

ACTING CHAIR HINOJOSA: You can just go ahead and have a little bit more if you need to finish.

MS. FIERST: Thank you. I appreciate it. We simply do not yet know the scope of the problem of alien harboring and trafficking, especially in light of the new Act's provision and amendments which makes the addition of specific guideline amendments, cross references, and offense characteristics premature. We just lack empirical data at this point to support the idea that the current guidelines are inadequate to serve the purposes of punishment, nor is there a reason to add a specific offense characteristic at this point, considering there are already nine
specific offense characteristics under 2(l)1.1.

And I would just like to end with a quote from the Commission's 15-year report, "A sentencing system that attempts to account for every conceivable offense and offender characteristic relevant to sentencing could quickly become unworkable. As the number and complexity of decisions needed to apply the guidelines increase, so do the resources required for investigations in sentencing hearings, as well as the risk that different judges will apply the guidelines differently."

As I indicated, that quote is from the Commission's 15-year report citing, in fact, a 2001 article by Professor Ruback and Commissioner Wroblewski. Thank you.

ACTING CHAIR HINOJOSA: Thank you, ma'am. Ms. Stauss?

MS. STAUSS: Thank you very much, Mr. Chairman and members of the Commission for giving me the chance to speak today. And I also congratulate you on the complexity of a
code that, as a victim service provider
delving into it for the first time in-depth in
recent weeks, really, as a victim service
provider, helps us to think when we're
advocating for sentences that will do justice
in the cases of our clients that there are
many more steps beyond just advocating for the
statute to determine what justice actually
will be served.

I think on this first question
about the alien harboring, it would be helpful
to understand the context of how this
provision got into the TVPRA. The original
version of the TVPRA that passed the House of
Representatives included a provision that
especially would have federalized all
pimping, regardless of whether there was
force, fraud, or coercion, in recognition by
those who supported it that many cases of
pimping it is very difficult to prove the
force, fraud, and coercion that occurs with a
crime and so that it would be better to punish
those all of those cases in recognition of the
severe harm that, in most cases, accompanies pimping.

Now, this version didn't pass, you know, I think the Senate, and those who were opposed to it really wanted to concentrate the federal resources on those cases that were human trafficking involving force, fraud, or coercion. But I think it helps to understand that context that the final result here with this alien harboring provision was a compromise that attempted to recognize those cases where there was an inherent imbalance of power between the victim, the prostituted person and the pimp because the victim was in a situation where they were undocumented, and so there was almost inherently a balance of power. And so it was a sort of compromise in order to federalize some of those pimping crimes or at least move in that direction.

I think harboring an undocumented person in order to exploit that person in prostitution is often committed simultaneous with sex trafficking by force, fraud, or
coercion. And proving the force or coercion necessary to convict under the sex trafficking crime is often very difficult; and, therefore, sex traffickers are prosecuted very often under other crimes, like this alien harboring provision.

For example, in a series of raids on Korean massage parlor-front brothels in the Washington area, my organization identified nearly half of the women on the premises as victims of trafficking under the federal definition that involves force, fraud, or coercion. But in those cases, the U.S. attorney was only able to achieve convictions under other crimes. In some cases, this is because the traffickers' exercise of control and power is hidden in those cases. The victims often tell us that they are very unhappy, depressed, and traumatized because of the continuous stream of unwanted commercial sex with different men. And the traffickers intentionally take advantage of the victims' undocumented status and exploit their pre-
existing fears of deportation and of immigration agents. And so even without voicing direct threats, traffickers do create a coercive environment in which women feel they have no choice but to continue in this situation against their will. I mean, we do believe that harboring could still reference Section 2(l)1.1 but that a special offense characteristic should be added adding two points to the base 12 when the crime involves organizing, leading, managing, or supervising the prostitution.

I just want to make a comment about a couple of the other items or issues for comment: the financial benefit crime, financial benefit from participating in a venture that engages in violations of certain of the trafficking and slavery offenses in Chapter 77. We would support applying guideline 2(h)4.1, and I think there's precedent for applying the same guideline as the underlying crime for this financial benefit. There's already a financial benefit
crime contained within Section 1591 that sex trafficking of a minor or by force, fraud, or coercion crime that was already on the books, and that financial benefit crime applied the same guideline as the underlying crime.

On the new crime, fraud and foreign labor contracting, those who engage in fraud and foreign labor contracting often are knowingly the first link in a chain of human trafficking, and so in that case would also favor referencing 2(h)4.1, but we would be comfortable with another guideline that would allow significant punishment of fraud and foreign labor contracting. This could potentially include the guidelines referenced by the Migrant and Seasonal Agricultural Workers Protection Act with a fraud-related special offense characteristic.

Just in closing, I wanted to note also that the Chairman's explanatory statement for the TVPRA characterized preying on mental illness and drug use or addictions as a form of coercion equivalent to human trafficking.
And while this wasn't an issue for comment, since I have a little bit more time I wanted to recommend adding those factors as a special offense characteristic similar to the concept of an undocumented person having an inherent power imbalance. The same applies when the victim has a drug addiction, so we would support adding that as a special offense characteristic, as well. Thank you very much.

ACTING CHAIR HINOJOSA: Thank you, Ms. Stauss. Mr. Song?

MR. SONG: Chairman Hinojosa and distinguished members of the Committee, Happy St. Patrick's Day. I see two of you got the memo. I don't know about the rest of you, but thank you for very much for the privilege to testify --

ACTING CHAIR HINOJOSA: The rest of us are relying on this.

MR. SONG: Oh, okay. We'll give you credit for that. Thank you so much for allowing me to testify today on behalf of the hundreds of survivors of trafficking and their
families that I've had the privilege of representing over, I can't believe it but it's been almost a decade now since I've been representing trafficking victims. And I've had the good fortune of representing trafficking victims before the Trafficking Victims Protection Act passed and after, so I have a good sense of what things were like prior to that act passing and what it's like now that we have the Trafficking Victims Protection Act and its numerous reauthorizations and amendments.

In preparation for my testimony today, I spoke to a few of my clients about their thoughts about what kind of sentences they would like to see. And just to give you an idea of how important sentencing is in this scheme of anti-trafficking work, I'd like to share one story of one of my clients. Since it is St. Patrick's Day, I'll call her Patty just to give her an identity. Obviously, it's a false identity. But Patty was trafficked to the United States from Saudi Arabia by a Saudi
princess, no less. She was brought to the Massachusetts area. Some of you guys may have heard about this case but I'm sure don't know the identity of my client.

She was enslaved in a domestic situation for a number of months before she felt like she was physically in danger and couldn't stand the situation anymore. In the dead of winter in Massachusetts, I don't know if any of you guys are from Massachusetts, she fled the house with the clothes on her back and shoes on her feet in the middle of the night. She was able to make it to a diner or restaurant and found good samaritans there that were able to help her. And I don't know how she was able to do this, but she was able to travel through the country working and surviving and then made it all the way out to Los Angeles.

Several years later, she was referred to me as a domestic violence victim who may have had some trafficking issues in the past. She was the victim of domestic
violence in traveling through the country to make it to Los Angeles. Anyway, she had children in her home country at that time still, and her trafficker had threatened, "If you ever do anything, if you ever escape, if you ever talk, I know where your children are, I know where they live, I have access to them, and I'm essentially going to hurt them or kill them," and she took these threats very carefully.

And, of course, one of the first things she asks me and many of my clients ask me is, "Can you guarantee the safety of my family, of my children, or even myself?" and I say, "Absolutely not. Nobody can do that."

But despite her fear and her concerns, she said, "You know what? I'm going to do this anyway," because when she escaped, she believed that this trafficker was trafficking other people or would traffic other people to the United States and continue enslaving people at her residences in the Massachusetts area and decided to go through with it anyway.
Anyway, so her report to law enforcement, to authorities, led to an investigation and prosecution. They did find that this Saudi princess was trafficking other people into the Massachusetts area in her residences and, after investigations and gathering evidence, there was a prosecution. Ultimately, the princess plead to, you guessed it, alien harboring and smuggling. You know, unfortunately, she was only sentenced to, if I remember correctly she had one of her houses confiscated, she had six months house arrest in one of her mansions, which was, I'm sure, horrible, and then she was going to be deported after that period. And then she was also going to pay restitution in significant amounts of money to my client and to some of the other victims, but really just pocket change to her.

When I told my client about the sentence and about this payment, she had a hard time breathing and started hyperventilating, and I thought, you know, it
must be because she's getting all this money
that she never imagined that she would ever
receive. But instead or rather it was because
she was so upset and so fearful about the
trafficker now being released to her home
country. And I still remember these words
vividly because she said, "That's exactly what
she told me was going to happen. She said if
I ever told police or reported to law
enforcement she said, `You know what? I'm
rich, I'm wealthy, I can buy my freedom," and
that's exactly what my client thought happened
in that case was that this person who had
trafficked her and enslaved her and others had
essentially purchased her freedom, and she was
devastated by this after risking her life and
her children's lives most importantly because
she didn't really care too much about her own
life but her children's lives.

And Karen took you back a little
bit about -- oh, I'm sorry. There's one thing
that I forgot to mention. And so at the very
end, I asked her, "Well, is there anything you
want me to tell the Commission?" because I
told her about this hearing, and she said,
"Tell them that all we want is a little bit of
justice," that that's all they're asking for.

Karen took you through a little
bit about the history about the TVPRA, but I
wanted to go back a little bit further so that
you understand where the victims are coming
from and the reason behind this act and what's
happened in this act. And I apologize if
someone of you are familiar with the
Trafficking Victims Protection Act, but I feel
like it's so important to understand the
background to these criminal provisions so
that we can appropriately sentence criminals
who are convicted of these crimes because, as
you well know, if we don't have a sentence the
conviction is really worthless or very
ineffective if we don't have an appropriate
sentence.

But the TVPA is, essentially, an
act in response to the federal government or
CIA report that some of you guys may remember
reporting that approximately 50,000 women and children and men were trafficked into the United States each year. That number has since been downgraded to maybe 14,500. So, anyway, my estimates are anywhere between 14,500 to 50,000 are still being trafficked into the United States, and it's a number that could increase because of the current economy.

But what was critical about the Trafficking Victims Protection Act was that it was an attempt to address human trafficking holistically by protecting victims, prosecuting traffickers, and preventing future trafficking. And the sentencing guidelines, although they also address the prosecution part of that, the intent of the Trafficking Victims Protection Act, I think they also go a long way towards protecting the victims who are enslaved but who also testify in some of these situations, further endangering themselves, in addition to assisting in prosecuting themselves.

And the new criminal provisions in
the Trafficking Victims Protection Act
dramatically improve the ability -- whoa. I
am over my time limit already. I totally
missed that. Anyway, I guess I'm the typical
lawyer that I like to talk, but I'll just
conclude because I have my recommendations in
my written statement. But I'll just conclude
by saying that I think the most important
thing that I'd like to express to you today on
behalf of my clients is that in addition to
being enslaved and trafficked in their
situations, they go through an incredible
ordeal and jeopardize not only their physical
and mental well being when they cooperate and
participate in that criminal prosecution but
also their families and also to just keep in
mind that all they're really looking for is a
little bit of justice. They're not expecting
a lot. Thank you very much.

ACTING CHAIR HINOJOSA:
Commissioner Howell?

COMMISSIONER HOWELL: The
Department of Justice has suggested with
respect to another law, a recent law that Congress passed involving the Child Soldiers Accountability Act that the Commission consider, it's a very intriguing idea, consider, rather than doing sort of a piecemeal approach to the Child Soldiers Accountability Act, as well as the new Trafficking Victims Act, that we take a broader approach and perhaps consider a guideline that specifically deals with human rights crimes, these new offenses and these laws, as well as other offenses that could be grouped under a human rights guideline.

And I know that, Mr. Koehler, you also talked about perhaps deferring some judgments on the Trafficking Victims Act from this amendment cycle to the next amendment cycle. That would give us time to actually consider this intriguing idea from the Justice Department to do a human rights guideline. I'm interested in the reaction of the victims representatives, as well as the Federal Defenders, about this idea of perhaps not
acting right now on these amendments, even though we have proposals to sort of respond to the directives and put some of the new offenses that have been created with referrals to current guidelines, what your reaction is to this other idea of creating a whole new human rights guideline where we could direct some of these new human trafficking victims act offenses and address them in a more holistic way. Could you just address that, if you've had time to think about it, if you have an opinion or not?

MS. STAUSS: I mean, I haven't had time to think about it beyond the last minute since you broached it to me for the first time, but I guess my question would be what qualifies as a human rights crime? Is it because these crimes have some type of international aspect? And I think, oftentimes, we see things that happen in an international connection violations of human rights, but if it's in the U.S. it's civil rights. What would define human rights
crimes, as opposed to other crimes that also
often do involve human rights violations?

COMMISSIONER HOWELL: That was one
of the questions we have to address, defining
what would be appropriate under this human
rights guideline.

MR. SONG: My point of view is I
would agree with the DOJ on deferring to the
next amendment cycle because I think there are
very complicated, difficult issues to address
and having more time to -- I don't see it as
anything as absolutely urgent here in amending
the guidelines, so I would support that.

I think your idea of coming up
with human rights guidelines is actually
really interesting and fascinating. I would
love to look at that and study that to see if
that would be the best way to handle some of
these new crimes because, for example, the new
foreign labor fraud provision or crime and how
to reference that. I was speaking to some
people about, you know, well, what do you guys
think about how we should reference this, and
we had the whole range from the fraud or theft
guidelines to the involuntary servitude,
bondage, or some kind of a combination, and
this is where [you] could come up with a
combination guideline because the foreign
labor fraud encompasses, you know, theft and
fraud from the very beginning. They're really
just committing fraud and stealing their money
up-front but then bringing them to the United
States, exploiting their labor, stealing their
labor if you want to look at it that way and
exploiting them. So it actually encompasses
both the theft and fraud and the labor worker
exploitation. So if we could get a guideline
that encompasses all of that, that would be
the ideal situation.

MS. FIERST: Again, just to wrap
up, we don't believe that any SOCs or cross
references are necessary to address the
congressional directive, which, again, just to
make our position clear, the congressional
directive suggested changes if the Commission
deems them appropriate. It was not a
mandatory directive to the Commission. But in any event, we believe that the Commission should take more time to gather data and to perform research to understand this issue a little bit more broadly. And if that included following up on the suggestions made in Mr. Koehler's letter and the U.S. Attorney's Office submission to the Commission, then that would be appropriate; but we just don't believe that that would be an appropriate action to take at this time.

COMMISSIONER HOWELL: Well, I take to heart some of the criticisms that you raised, as a practitioner sitting in the courtroom, about the difficulty of applying cross references, the additions of SOCs, and the kind of invitation to litigation that can be, and some of the confusions. I think every commissioner is really well aware of that, which is part of the reason that perhaps avoiding that and looking at a new human rights guideline that would avoid some of the cross references would more target
appropriately some of these offenses is something that, you know, I just really wanted the reactions to how people would react to that because it would avoid some of the criticisms that you appropriately pointed out about some of the proposals that we've actually put out for comment.

Thank you all very much.

MR. KOEHLER: I had a brief comment on the one issue, and I didn't get this far in reading my testimony here. But the foreign labor fraud new provision that's in the statute, Section 1351, we mentioned in our letter potentially looking at 2(h)4.2 or 2(h)4.1. There's also 2(h)1.1, violations of individual rights, that might apply, and that might also serve as a starting point for the guideline that you were discussing that would be more of a broader type of guideline. And perhaps you could have adjustments in such a guideline that would account for the number of victims, as well as the type of conduct at issue.
But I don't think that that particular guideline or that type of an arrangement would fit better with harboring in furtherance of prostitution better than the harboring guideline would if you merely added a two-level upward adjustment for harboring that furthers adults prostitution or a four-level upward adjustment that would involve harboring that furthers child prostitution when the person is an organizer, leader, manager, or supervisor.

COMMISSIONER HOWELL: Thank you.

MR. KOEHLER: Thank you.

VICE CHAIR CASTILLO: I would be interested, as part of this continued study in this area, how the Commission could get a handle on the deterrent value of increasing penalties in this area and, in particular, how do we go about protecting the family members of victims who reside in other countries, and that seems to be part of what is going on here in terms of ensuring that the victims do serve in these illegal manners in the United States.
So any ideas or thoughts on that?

MR. KOEHLER: I assume you're addressing me with that?

VICE CHAIR CASTILLO: Well, you come to mind, Mr. Koehler.

MR. KOEHLER: Okay. In terms of deterrence, I think deterrence is a very difficult thing to measure in terms of the sentencing guidelines, and I'm not sure there is an appropriate way to measure it other than looking at recidivism rates. But my thought in terms of protecting the public is incapacitation rather than deterrence, and that's a factor that 3553 clearly encourages both sentencing judges, as well as the Commission, to consider when promulgating the guidelines.

And when you're dealing with folks who are playing a superior role in an alien-smuggling enterprise and harboring enterprise who are furthering prostitution, clearly those people deserve incapacitation for a longer period of time. And the same is true with
folks who traffic obviously, which is why those guidelines are so much higher in the first place.

Incapacitating persons for longer period of times certainly does not protect the trafficking victim from action by a proxy for the defendant. But at the same time it puts the defendant out of commission for a longer period of time and prevents them from re-victimizing these people or victimizing new people while they're incapacitated. So it has value in that sense.

ACTING CHAIR HINOJOSA: Vice Chair Sessions?

VICE CHAIR SESSIONS: Just to follow up with a question that Ruben just asked. I'm particularly asking practitioners. The defenders have included in their submissions a study, in fact a series of studies, which indicate that recidivism rates are affected, or deterrence, essentially, is affected or impacted by the certainty of punishment but not the length of punishment.
In other words, once you get past a certain period of time it doesn't make any difference whether you give a sentence at that point or far into the future.

And then the issue of deterrence, you know, you're a practitioner, in particular, Mr. Song, do you agree with that concept, or is that something which is disagreeable or you do not agree with?

MR. SONG: I've learned to agree with the government, for the most part. Just kidding. No, I do happen to agree with them on this point, but also deterrence is so incredibly difficult to measure and to see the effectiveness, but I would agree that just incapacitating certain traffickers is extremely important. And I don't have the studies to show that the length of sentence is not as important, but I know that I'm involved in a sex trafficking prosecution right now where we're waiting for a number of defendants who have been convicted on sex trafficking and actually harboring, both charges. But I know
that my clients are on pins and needles about what the actual sentences are going to be, so for them it's incredibly important.

But I'd also say that, and I don't have any evidence and I certainly can't prove this, but my experience with trafficking cases has been some of these traffickers calculate how much time they could possibly do for the amount of money they can make. And, again, I can't prove it. That's certainly my disclaimer. But when you think about the amount of money, especially in sex trafficking cases, that you make on a daily basis prostituting minor girls or adult women, they make thousands of dollars a day. And I can't, you know, prove it again, but I'm very confident that a lot of these traffickers are calculating, they're doing the math. They're not stupid people. They're doing the math and saying, "Okay, I can make X amount of money, and I can possibly go to jail for X amount of time. Well, you know what? That's like working for three or four years and making
hundreds of thousands of dollars or whatever
that I'm going to sock away in whatever
country so that nobody can access it even if
I do get caught and get convicted," etcetera.
But in some cases, like the Saudi princess
who's worth, I'm sure, quite a bit of money,
she did six months of house arrest and then
got deported for basically enslaving domestic
workers in her house for who knows how long
because we only caught her for a short period
of time.

So I would say I don't have the
evidence, but I believe that the length of the
sentence is incredibly important just for the
victims. Again, they're not asking that we
execute the traffickers or put them in jail
for the rest of their lives, but they're
asking for a little bit of justice, a little
bit of fairness. If you enslave me and other
people, it's only fair that you should be
incapacitated for a certain amount of time,
and I do believe, you know, just based on my
own experience, that the length of sentences
does have an impact definitely on my clients, on the victims, but I think on the traffickers as well.

MS. FIERST: If I could actually just add to that. With all respect for Mr. Song's experience, I also have had my own experience representing defendants in these cases and defendants who are not originally from this country in general, and my experience often is that they are not very familiar with, nor do they well understand the laws of this country. They don't understand mandatory minimum sentences, they don't understand the length of sentences, they don't understand enhancements, criminal history, and many of the facets of the sentencing guidelines, which, of course, practitioners themselves have their own issues with. And so while some of them may, in fact, take these things into consideration when they're committing their offenses, I know there's also another segment of the population which does not.
And with respect to the types of cases that Mr. Song is referring to, I don't know the facts of his Patty case, although it sounds to me from the facts of the case that that will be a case where there would be an increased base offense level because of coercion and threats and there would be additional enhancements based on the number of people trafficked. But, again, I was not part of that case, so I don't know how the sentence ended up where it did. But, certainly, there are very lengthy sentences and very significant mandatory minimums that are available in the egregious cases, in the cases involving minors, in the cases involving large numbers of people being trafficked into this country, and there are already the SOCs and the cross references and the mandatory minimums available to make sure that those people do receive significant punishment.

ACTING CHAIR HINOJOSA:

Commissioner Wroblewski?

COMMISSIONER WROBLEWSKI: Thank
you. And thank you all for coming and


testifying. First, Ms. Fierst, thank you so


much. There's nothing an author likes better

than to be quoted, and I look forward to

working with you and the other community and

public defenders on the rest of what was
discussed in that article, which was looking

at overall simplification of the guidelines

and reform and the presumptive nature of the

guidelines.


    Ms. Stauss, I just want to sort of

bring this back for a second because we're


talking about trafficking cases and force
cases and coercion cases, and it seems to me

the one area that I think that we're talking

about perhaps amending this year is the

harboring guideline, the cases involving

harboring where that's the offense of

conviction, and there's the added aggravating

factor that the defendant was an organizer or

a leader in a prostitution scheme. Am I

right, Ms. Stauss, that all you're suggesting

there is going from a base offense level of 12
to an offense of two more levels? You suggested a two-level enhancement if the person is an organizer or leader and there's prostitution involved; is that what we're talking about?

MS. STAUSS: I think, you know, my understanding of the offense levels might not be as deep, certainly, as those who are in the criminal court everyday. But we definitely are suggesting that, you know, and my written testimony suggested that for us it's not that important, and I think for many victims they are not paying attention to, you know, the name of the index of the sentence but, rather, that there be an appropriate sentence.

So as I said in my written testimony, whether we go with 2(1)1.1 and add points to that or go to one of the other offenses, the idea is that we support broadly increasing the penalty in those cases where the harboring is in furtherance of prostitution with this understanding that, while the description of the crime doesn't
involve force, fraud, or coercion, that is the reasoning for adding the increased penalty because there is an inherent power imbalance between the victim and the person harboring when the victim is an undocumented alien.

COMMISSIONER WROBLEWSKI: Right.

But the result in that kind of case would not be taking someone who would normally be sentenced to seven years and adding another two years. We're talking about someone who might be sentenced to six months home confinement and making it a split sentence in the example that we're talking about, not that there's a conviction for 1591 or other trafficking sets, for just harboring.

ACTING CHAIR HINOJOSA: Well, what this hypothetical ignores is that there would have been an enhancement under Chapter 3 for the role offense, so it wouldn't just be 12 plus 2. There would be a role enhancement of up to four points possibly, depending on how many people were involved. And so for someone who's not familiar with the guidelines, it
would be unfair to not indicate to them that there is an increase for a role offense in every case an enhancement that would apply in any case where somebody is an organizer, manager, supervisor, or leader. And then we could have a specific offense characteristic that would be plus two, but you're not just stuck within that 1.1. There are some other adjustments that would apply to somebody who is an organizer, leader, manager, or supervisor.

MS. STAUSS: Right. And our understanding, in many of the cases that we see that are difficult to bring as 1591 cases, often there is some element of fraud and understanding that there would also be an addition of four points for fraud, and so with the two points for the prostitution and the four points for the fraud you get up to 18, which was consistent with, I believe, the 2(g)1.1 with cases involving fraud also so that we would be arriving at the end result. And, you know, whether it's through 2(l)1.1 or
2(g)1.1, I don't think --

ACTING CHAIR HINOJOSA: Your point is you would like --

MS. STAUSS: -- one way or the other.

ACTING CHAIR HINOJOSA: Your point is you would like to see that taken into account with regards to an increase in the sentence?

MS. STAUSS: Right.

MS. FIERST: But if I might, if I might just briefly, with respect to an inherent imbalance of power, again with respect to Ms. Stauss' experience, there are times where there are willing participants in the prostitution trade. We're talking here, it seems to me --

ACTING CHAIR HINOJOSA: Well, it depends on how you define willing in the sense that some people are so desperate to come to the United States that they would be willing to subject themselves to something. You know, having experience just like I do with regards
to cases that are immigration cases, there's
different levels of willing participants.

   MS. FIERST: Absolutely,

absolutely, your Honor. But keep in mind, of
course, that if this is somebody who is so
desperate to come to the United States that
they're willing to engage in prostitution,
then this is potentially a case that could be
charged under a 1328 where someone is imported
particularly for that purpose. If you have a
good prosecutor, they can prove fraud in a
case where there's an unwilling participant,
an inherent imbalance of power like Ms. Stauss
is talking about. You can prove fraud,
coercion, duress under any -- in other words,
we're not simply talking about fraud, we're
not simply talking about coercion, we're not
simply talking about threats. The possible
enhancement is broad, and so a prosecutor with
those facts where there is this inherent
imbalance of power that she's referring to
based on her experience could prove those
facts in a 1328 or a 1591 conviction. There
are already enhancements, we believe, that address these issues and with enhancements for the number of aliens who are participating under 2(1)1.1. You already can reach that manager, organizer, or leader level participant so that I do think that Mr. Song's experience in the Patty case is really such an outlier based on the facts that he's referring to.

ACTING CHAIR HINOJOSA:

Commissioner --

MS. STAUSS: Sorry, I just wanted to respond. Is that okay? The 1328 crime requires an importation, a connection to the importation of the person that I think very often we're seeing is not the case. It's not necessarily that the person experiences fraud in their coming to the United States but that they may experience fraud in the offering of a position, if you will, in a brothel where they're told that the conditions will be, you know, that there may be particular conditions and then the conditions are far worse than
they're told, and they're desperate to get out, but they don't feel that they're able to get out.

ACTING CHAIR HINOJOSA:

Commissioner Friedrich?

COMMISSIONER FRIEDRICH: Yes. Mr. Koehler, you suggested in the alien harboring context adding a SOC to 2(l)1.1 for cases where the defendant played an aggravated role. Is that because you don't believe certain defendants would qualify for an aggravated role enhancement at a 3(b)1.1 where their aggravated role was with respect to the prostitution as opposed to the harboring? Is that --

MR. KOEHLER: No. I'm talking about any defendant who is convicted under Section 1324 and to whom 2(l)1.1 applies and who receives the 3(b)1.1 adjustment for being a manager, organizer, leader, or supervisor in the criminal activity, whether it's the prostitution or the harboring offense. If somebody is an organizer or leader of a
harboring offense and the harboring involves prostitution and this organizer or leader has reason to know about it, they're responsible for the conduct of their subordinates. They're the people who are in a position to stop that activity and either limit the offense to harboring or disband it all together. And so for that, they ought to be held responsible in that position for the harboring.

Doing so, you know, this is much less than the trafficking that they're not convicted of or the involuntary servitude that they're not convicted of. The offense level here is much lower in that sense. So it's appropriate to impose an adjustment upward from what is an ordinary harboring sentencing guideline level to account for the prostitution activity. And it's not just important in terms of incapacitation, it's also important in terms of promoting respect for the law. You know, promoting respect for the law is discussed in 3553(a) is not just
about the respect of the law by a person who might violate the law but by the person who has been victimized by the person who violates the law. Respect for the law among the public is just as important in that sense, and this would further that goal.

ACTING CHAIR HINOJOSA:

Commissioner Reilly?

COMMISSIONER REILLY: Since you mentioned victims, I wanted to mention, obviously, the emphasis that's been placed over the last number of years about the victims. I'm curious what your experience is with regard to what the TVPA says that it assures in terms of service, social services. What is being provided? Are these people being adequately taken care of in that regard, the victims?

And the second part of the question would be are those who are seeking a safe harbor because they do fear for their lives, where are we putting them?

MR. KOEHLER: I'm afraid I would
have to punt that one over to the folks --

COMMISSIONER REILLY: I mean, are they being put in the victim witness program?

MR. KOEHLER: There are trafficking victim provisions that enable trafficking victims to get visas to come into the United States, both T visas and U visas for victims of certain types of crime. And so that is a provision that, through certification by the lead officer of a law enforcement agency within the discretion of CIS, those people can be given a visa to stay in the United States. I think that Ms. Stauss or Mr. Song might know more about the specifics of how that would work than I would.

ACTING CHAIR HINOJOSA: Wouldn't that be the exception rather than a rule in all likelihood to get deported?

MS. STAUSS: Well, in order to qualify for the T visa or the U visa, the victim does also have to be willing and able to participate in any investigation or prosecution that's brought. I'm sure that
Charles will weigh in here, too.

As far as the services that are available for those who do agree to participate in an investigation or a prosecution, which is certainly not all of the victims who are foreign nationals, there are services available. We've been advocating that they be for a longer term because, in many cases, the services last for a certain period of time that is not as long as it takes for these survivors to oftentimes regain their balance, especially when they're often coming from situations of economic desperation, lack of education.

I just want to make one other point, though, that, while we've talked a lot about the alien harboring, the issues for comment today cover crimes that apply to all victims of trafficking, not just foreign nationals but also U.S. citizen victims of trafficking, and that's an area where I think we've been really remiss in providing services to survivors where we don't have any special
funding for specially-created programs to serve U.S. citizen victims of trafficking. And so that's something that many members of the victim service community have also been advocating for, in addition to lengthening the amount of time and the availability of assistance to foreign nationals.

MR. SONG: My short answer to your question is almost. We provide quite a bit of services to trafficking survivors in the United States. I would actually say, and I don't know, Karen, if you'd agree with me, but I think we actually have the best trafficking legislation in the world. We're always consulting with other countries about things that we can do. States have their own trafficking legislation, but they can provide housing, medical services, psychological services.

I think one area where we are most lacking right now are services, and I think, Commissioner Castillo, I think you mentioned this about the family members, protecting
family members. I think where right now we're most lacking in services or benefits to survivors is to their family members back home because, you know, my view is the only real way to protect somebody's family members is to get them over here as quickly as we can because the longer they stay there, I mean we can't have, you know, we can't trust other law enforcement or government to protect them. We can't expect ICE or FBI or the State Department to protect them abroad.

The way I see it, from a victim's perspective, is the only real way to protect them is to get them over here as quickly as possible, hopefully, definitely before trial starts so that the defendants don't know who's testifying and have more incentive to silence them or obstruct justice. But, anyway, that would be my comment to that question.

ACTING CHAIR HINOJOSA: Thank you all very much. We certainly appreciate your time and your contribution to our process here.
Our next panel is entitled "Other Guideline Amendments," which gives you a free-for-all with regards to whatever you want to discuss but not really. Our first panelist is Ms. Suzanne Ferreira who is a Supervising U.S. Probation Officer for the Southern District of Florida, and she currently serves as a chair and 11th Circuit Representative for the Commissioners' Probation Officers Advisory Group.

Mr. Craig Magaw is the Deputy Assistant Director of the Office of Investigation of the U.S. Secret Service. He has had 22 years service with the Secret Service, and he is a member of the Elite Counter Assault Team and a member of the Presidential Protection Division.

Ms. Donna Lee Elm is a Federal Public Defender in the Middle District of Florida. Previously, she served in the Federal Defenders Office in Phoenix.

And Mr. Kenneth Linn is the Chairman of the Federal Chapter of CURE, which
stands for Citizens for the Rehabilitation of Errants. I hope you don't include us in that. And you're also President and CEO of Commonwealth Management Services Incorporated in Florida.

And we'll start with Ms. Ferreira.

MS. FERREIRA: Good afternoon, Judge Hinojosa and Commissioners. Thank you for the opportunity to testify here today on behalf of the Probation Officers Advisory Group. I'm going to present the group's comments as we have set forth in our position paper, or at least as much as my seven minutes will allow.

With regard to Identity Theft Restitution and Enforcement Act, there were a number of factors under consideration for amendment. The level of sophistication and planning involved in the offense, the group's position of the proposed amendment at 2(b)1.1 includes language under the sophisticated means definition regarding a scheme involving computers to conceal the identity or
geographic location of the perpetrator. The
group recommends this language should include
using computers to conceal not just the
perpetrator but the offense itself. It was
suggested that language similar to the
layering language in the money laundering
guideline might be appropriate.

The group also agreed the two-
level enhancement for sophisticated means is
sufficient to capture this factor and, in most
cases, the dollar amount of loss drives the
offense level. The floor of level 12, which
was instituted in 1998, is no longer
sufficient based upon the serious nature of
many of these offenses. The group agreed that
the floor should most likely be raised, but a
review of sentencing data related to the
frequency of the application of this floor
might be helpful in making that determination.
The group unanimously agreed the language at
3(b)1.3 should be changed to unequivocally
include a person who has self-trained computer
skills as one who has a special skill.
With regard to the factor whether the offense was committed for purpose of commercial advantage or private financial benefit, the current language at 2(b)1.1, 2(b)1.5, 2(b)2.3, 2(b)5.3, and 2(h)3.1 adequately addresses the factor described in Section 209 B2 of the Act. There was some concern raised, however, in some inconsistent application and the retail value of low-quality and high-quality fakes, specifically with regard to offenses covered under 2(b)5.3, copyright infringement offenses.

The next factor under consideration is the potential and actual loss resulting from the offense, including the value of information obtained from a protected computer, regardless of whether the owner was deprived of the use of the information or the information obtained constitutes a trade secret or other proprietary information, the cost the victim incurred developing or compiling the information.

Regarding the proposed amendment
at 2(b)1.1 Commentary Note 3, the group agreed that option two was the better choice. The first option was determined to be problematic in terms of placing a value on proprietary information.

Option two, on the other hand, uses a dollar amount that is more likely to be available from the victim. Overall, a broader application is preferred as a better way of determining harm.

With respect to the first and second issues for comment regarding information from a protected computer, we concluded that, as currently written, the guideline is not sufficient to capture loss. If option two, as described previously, was adopted, however, it would be sufficient in conjunction with Application Note 19, which outlines departures.

With regard to question three, the group agreed that a victim who suffers pecuniary harm but is immediately reimbursed by a third party should be considered a victim.
for purposes of the SOC for the number of
victims, and their reimbursed losses should be
included in the dollar amounts under 2(b)1.1
(b)1. In addition, the group agreed that
victims with unidentified and/or non-pecuniary
harm are being overlooked in many cases.
Frequently, these individuals may not know
they were victimized. The investigation into
the illegal activity ceases before potential
victims are identified and sometimes even
notified. And other losses which may be
sustained or have yet to be sustained are not
captured.

The group would urge a more broad
definition of victim in order to better
capture the size or extent of the offense. A
special rule similar to that found at Section
2(b)1.1 Application Note 4 may be appropriate.
Where there is a theft of a large number of
credit card numbers or a databases access, the
potential victims may need to be more vigilant
in monitoring their credit, even if they did
not sustain any part of the actual loss.
In sum, victims of crimes who did not sustain a pecuniary harm oftentimes sustain non-pecuniary harms that are not being captured. In addition, the group unanimously concluded that 3(b)1.3 should be amended to unequivocally include a person who is an officer, employee, or insider of a business who participates in any offense involving proprietary information and the employee had access to that information.

With regard to the factor whether the defendant acted with intent to cause either physical or property harm in committing the offense, the group concluded the factors [are] adequately addressed by other enhancements. With regard to the extent to which the offense violated privacy rights, the group declined to make a recommendation based upon our negligible experience with these kinds of offenses.

With regard to the factor the effect of the offense upon the operations of an agency of the United States government,
state or local government, we agree that an upward departure provision will adequately address this factor and is the better option, as the group agreed we rarely or never see cases where this factor even applies.

With regard to the factor whether the defendant's intent to cause damage or intent to obtain personal information should be disaggregated and considered separately from other factors set forth in 2(b)1.1, the group agreed that the intent to cause damage or intent to obtain information should be disaggregated but not solely in the context of 18 USC 1030 cases. Our experience has shown that the government infrequently charges under 18 USC 1030.

With regard to the factor whether the term "victim" is used in 2(b)1.1 should include individuals whose privacy was violated as a result of the offense, in addition to individuals who suffered monetary harm as a result of the offense, the group agreed that the term "victims" should include individuals
who suffered non-pecuniary harm, as previously recommended.

The group agreed that the definition of reasonably foreseeable pecuniary harm should not be amended to include the cost to the victim of correcting or repairing the harm incurred because it would be too difficult to determine, would result in inconsistent application, and would create evidentiary issues which would complicate the sentencing process.

With regard to whether the defendant disclosed personal information obtained during the commission of the offense, the group agreed there should be an increase of charged offenses other than 18 USC 1030 and 119 where personal information is made publically available. Crimes involving victims of identity theft should be punished more harshly if the information was not just obtained but otherwise disclosed. The disclosure could be defined as made publically available, as described at 2(h)3.1, Subsection
(b)2B.
With regard to the Ryan Haight Online Pharmacy Consumer Protection Act of 2008, the group agreed that offenses involving Schedule II substances are not adequately addressed by the guidelines. It was the consensus that the maximum base offense level of 20 for offense involving Schedule III should be eliminated entirely, and the offense level increases should mirror those for Schedule II substances. A base offense level of 20 applies to 40,000 or more units. With the advent of online pharmacies, the amount of Schedule III substances involved in an offense has oftentimes exceeded a million dosage units. Even before online pharmacies, we were seeing that level of dosage units in local pharmacies in certain areas of the country.

With respect to Schedule IV and V substances, the group does not have enough experience with cases involving these substances to render an opinion. Because of the low threshold for Schedule III substances,
many reach the maximum level for Schedule III without even consideration of any Schedule IV or V substances, and many of those types of substances, including cough medicines, were handled as civil licensing violations rather than criminal prosecutions.

And the group also agreed that offenses involving Schedule III hydrocodone should not be treated differently than other Schedule III substances. The group was reluctant to recommend changes to the guidelines based on the current popularity of a substance. It seems that lifting the base offense level threshold of 20 for Schedule III would be the better approach and would obviate revisiting the issue when the next Schedule III substance achieves an alarming level of abuse.

I see my time is up. I have several more issues. It's presented in our position paper. I can rely on that, if you'd like.

ACTING CHAIR HINOJOSA: You can
finish, if you'd like.

MS. FERREIRA: Okay. The next issue was the Drug Trafficking Vessel Interdiction Act of 2009. The group reviews the proposed amendments and agree that 2(b)1.1 (b)1B would adequately address the use of submersible vessels. We consulted with probation officers in the Middle District of Florida, which is the only district known to have had any involvement with these type of cases. They agreed that using a new guideline under 2(x)7.2 is preferable to using 2(x)5.1. The use of [a] specific guideline is less problematic than choosing an analogous guideline which invariably leads to strong disagreement.

In addition, the probation officers in that district strongly urged the Commission to consider using a higher base offense level under 2(x)7.2. These particular vessels are invariably used for drug trafficking. The problem becomes when they are scuttled. The evidence of drug
trafficking is oftentimes lost. It's a very dangerous situation for the U.S. Customs agents to try and retrieve this evidence in order to successfully prosecute the cases. So they encourage the Commission to consider using the new guideline with a high base offense level that would incorporate the factor that this is most likely used in a very serious criminal enterprise and, in addition, that some of the factors utilized or recommended as departures would be more appropriate as SOCs. The failure to heave to and the attempt to scuttle the vessel, those will invariably happen in every one of these cases. So the officers who have had experience with this recommended that those be specific offense characteristics rather than departures.

I have a lot more to go on. Do you want me to continue or . . .

ACTING CHAIR HINOJOSA: You have a lot more?

MS. FERREIRA: Well, you had a lot
of issues this year. You kept us very busy.

ACTING CHAIR HINOJOSA: Just pick the ones that you really want us to hear.

MS. FERREIRA: Okay. How about --

ACTING CHAIR HINOJOSA: Verbal statements on rather than just the written statements.

MS. FERREIRA: The William Wilberforce Trafficking Victims Act. Regarding the conformity between the guidelines applicable to persons convicted of alien smuggling and the guidelines applicable to persons convicted of promoting a commercial sex act, the group agreed a cross reference in 2(1)1.1 to 2(g)1.1 and 2(g)1.3 would sufficiently address those concerns. It would also provide conformity and ease of application. Probation officers agreed that a cross reference is a much easier application.

With regard to how the aggravating role factor for these types of offenses should be incorporated, the group considered the
option of creating an SOC but found that problematic since aggravating role is not normally addressed as an SOC. Alternatively, the group suggested expanding the language in 2(g)1.1 in the Commentary Note 3 to include an instruction for these types of offenses that the organization may be considered otherwise extensive for purposes of applying 3(b)1.1.

I think the concern there is it may be difficult to prove the number of participants. The group suggests adding a similar application note to 2(g)1.3. As to whether Appendix A should be amended to refer to the new offenses under 18 USC 1593(a) and 1351, the group agreed that any offense which can be referenced in Appendix A to a specific guideline provides more consistency and ease in application.

With regard to commission of offenses while on release, the group agreed that the new language and additional examples provided help to clarify the application note without changing the substance of the rule.
With regard to counterfeiting and bleach notes, the group reviewed the proposed changes at 2(b)5.1 and the application notes and agreed the changes are clear, easily understood, and should help resolve the issue.

That's it. I thank you for this opportunity.

ACTING CHAIR HINOJOSA: Thank you.

Mr. Magaw?

MR. MAGAW: Good afternoon, Mr. Chairman and distinguished members of the Commission. On behalf of the men and women of the Secret Service, it is my pleasure to speak to you today to discuss the Commission's proposed amendments to the sentencing guidelines for offenses involving counterfeit barrier obligations of the United States.

Counterfeiting of money is one of the oldest crimes in history. At some periods in history, it was considered treasonous and even punishable by death. During the American Revolution, the British counterfeited U.S. currency in such large amounts that the
currency soon became worthless. During the Civil War, one-third to one-half of the currency in circulation was counterfeit. As a result, the Secret Service was established in 1865 to suppress the widespread counterfeiting of the nation's currency.

Over the past 144 years, our mission has expanded to provide broader protection of the U.S. financial systems by investigating additional crimes, such as bank fraud, identity theft, access device fraud, computer fraud, and other cybercrimes.

However, the investigation of those who seek to counterfeit U.S. currency still remains a top priority for the Secret Service.

Counterfeit U.S. currency can be produced using a variety of methods. One method involves traditional printing process such as offset printing, which is one of the same methods used by the Bureau of Engraving and Printing when producing genuine U.S. currency.

Another method is a newer
technology-based process called digital imaging. A counterfeiter who uses offset method requires technical expertise in printing and the ability to use specialized equipment, such as a printing press, plates, and negatives. This type of counterfeit operation typically yields large quantities of counterfeit notes and can only be accomplished by a small number of sophisticated criminals. However, the Secret Service has observed over the last 15 years counterfeiters having changed their primary method from manufacturing to digital imaging. This newer method of manufacturing requires only minimum technical knowledge and access to scanners and printers easily available at local retail stores. Therefore, this shift to digital imaging manufacturing has now enabled a larger number of individuals to engage in criminal behavior.

In recent years, the Treasury Department has taken significant steps to defeat the modern-day counterfeiter. In
addition to the sophisticated printing methods, the Treasury Department has integrated new security features known as “distinctive counterfeit deterrents.” These include watermarks, micro-printing, security threats, different colored ink designed to protect the integrity of our currency while complicating the counterfeiting process. The Secret Service continues to work to stay ahead of modern counterfeiting operation through its involvement in currency design process, and it closely works with BEP, the Federal Reserve Board, and the Treasury Department. Today's counterfeiters are changing their manufacturing methods to incorporate the Treasury Department's distinct counterfeiting deterrents and distinct paper into their production methods to generate highly-deceptive counterfeit notes. In one such process, the counterfeiter takes a low-denomination genuine U.S. note, usually a $5 bill, removes the printed ink through a labor-intense process commonly referred to as
bleaching. This bleaching process creates a blank note of genuine U.S. currency paper that retains many of its distinctive counterfeit deterrents.

The counterfeiter then transfers an image of a higher denomination U.S. note, usually from a $100 bill, onto the bleached genuine paper. Color printers are the most common device used to transfer counterfeit images to genuine bleached paper, but counterfeiters can also accomplish this through more traditional offset printing methods. In either circumstances, the final product is an extremely deceptive counterfeit bill that blends the unique feel and features of genuine notes with a counterfeit image.

The Secret Service has observed that counterfeit notes produced on bleached paper are both a domestic and international concern. Counterfeiting operations based in Columbia, Nigeria, Italy, North Korea have all produced significant quantities of counterfeit notes that were printed on bleached genuine
U.S. currency. The use of genuine U.S. currency paper and the production of counterfeit obligations has presented some unique issues regarding the current counterfeit guidelines.

The current guidelines found at 2(b)5.1 appear somewhat ambiguous as to which guideline applies when an individual is being sentenced for counterfeiting activity related to bleaching. As the Commission is aware, several federal courts have resolved differently the question of whether offenses involving bleach notes should be sentenced under 2(b)5.1 or 2(b)1.1. As a result, some defendants convicted of bleach note counterfeiting receive lower sentencings from the courts than defendants convicted of less sophisticated counterfeiting methods. The proposed amendments should effectively respond to the concerns expressed by federal judges and members of Congress to provide much-needed clarity in this area.

The Secret Service fully supports
the proposed Sentencing Commission changes to 2(b)5.1. The Secret Service believes that currency illegally produced on genuine U.S. paper is counterfeit. Moreover, defendants who bleach genuine U.S. currency paper typically manufacture a highly-deceptive counterfeit note that is easier to pass. These counterfeiters rely on the distinctive counterfeit deterrents and unique feel of genuine U.S. currency paper to create counterfeit currency that is often difficult to detect and identify. As such, bleached note counterfeiters should be subject to the sentencing provisions governing counterfeit offenses.

The Secret Service feels strongly that individuals engaged in counterfeiting, regardless of the method they choose, should be treated with parity in sentencing. Furthermore, the Secret Service feels the potential increase in prison sentence under the proposed amendment to 2(b)5.1 will present not only a deterrent to those considering
engaging in counterfeiting U.S. currency for the first time but also for those already previously convicted of counterfeiting offenses who may undertake such criminal activity at a later date. Therefore, the Secret Service is pleased that the Commission is considering the proposed amendment to the counterfeiting sentencing guidelines.

Mr. Chairman, members of the Commission, I appreciate your time today and look forward to speaking to you [on] this issue.

ACTING CHAIR HINOJOSA: Thank you, Mr. Magaw. Ms. Elm?

MS. ELM: Thank you. Chairman Hinojosa and Commission members, I am very pleased that the Commission is taking an interest in hearing from the District where the boat cases are filed in the United States, and I'm pleased that you recognize the importance of knowing from the local district what the facts are about these cases.

I am the Federal Defender in
Tampa. Tampa is the only court where the Department of Justice brings its boat smuggling cases. They can bring them at any court, but they do bring them in Tampa, so we're very familiar with them.

I also want to note that I was a public defender for 18 years in Arizona. Arizona is one of the four states plagued with the border tunnel issue, a matter that will become important shortly.

Let me talk about the semi-submersibles. They are manned usually by one captain. His role is, essentially, he has the GPS and once a day he gets a radio call where he gets new coordinates and he proceeds. That is, essentially, what he does. He will also drive the ship.

There are usually three crew members. One is a mechanic. The other two are simply unskilled labor who will also drive the ship spelling the captain. Those crew members are usually paid only about $5,000 to $10,000 for this very life-endangering trip.
that they take. They are generally poor fishermen with family to support who live in very bad financial situations and are essentially mules being told where to go, what to do, and how to take things.

The subs themselves or semi-submersibles are very risky boats to take out onto the ocean. They're constructed often of fiberglass and wood. Recently, we've seen some with steel. And they're often leaky. They don't seal things well, and boats have been known to go down even more frequently than just what is reported by the Coast Guard. And those people are lost. The Coast Guard is not there to save them.

The technology that they have is not sophisticated. What we see is a GPS, a radio, an engine, you know, that runs the screw. And it is very little else.

Last Friday in Tampa in a case, we had a special agent of the Coast Guard testify about what it's like in the submersibles, and I will tell you some of the information he
gave us, which is consistent with what we have learned from our clients, and that is he called it an arduous and dangerous journey. The higher-ups exploit the crews knowing how compelling the money would be. I echo Chairman Hinojosa's comments that some people are so desperate in their financial situations, they're willing to undertake things that are illegal, unpleasant, or dangerous. And our individuals who we represent are finding themselves in that position, too.

There's very little air inside these tin cans. There's usually only two ventilation holes, and they don't necessarily supply enough air for inside. Additionally, they're not allowed out, they're generally not supposed to be out of the boats, so they're stuck in there for days.

The engine is inside. It is loud. It is hot. It rattles around and sometimes produces exhaust fumes that can be poisonous. It also takes up some of the oxygen.
So with all of this, plus the heat
of going through the tropical waters for days
and being stuck in there, it is a terrible
thing. And it also reeks. There is no
bathroom, no veritable pot. So this is what
they're traveling in. It's important to note
that the semi-submersibles are used to go
below the surface to try to avoid detection in
smuggling.

Now we come to the tunnels. The
tunnels are used to go below the surface to
try to avoid detection in smuggling. One by
land, the other by sea. Many tunnels run from
the United States into Mexico and are used to
move large quantities of contraband, like the
semi-submersibles. Those tunnels are believed
to have been financed because they cost
roughly a million dollars a piece, financed by
the drug cartels to move their stuff. They
are sophisticated. Many of them have
ventilation systems, phones, electricity and
lights. Some of them have tracks where they
can move with carts the drugs down. We have
ones that are built so big that Humvees can
drive through them. These are rather
substantial productions underneath the earth.
And instead of having 60 to 100-foot boats
manufactured, we have one tunnel going into
San Diego that was discovered that was a half-
mile long. They're given names: the Grand,
the Taj Mahal. Those are descriptors we could
never apply to our semi-submersibles.

Prosecutions also in that statute
do not involve the mules. What it is aimed at
and what is being punished are the people who
fund these, the people who possess them on
their property, the people who build them.
That is what those go to. And those people
are higher up the food chain than, for
instance, our poor fishermen who are being
paid the $5,000 to go aboard the boat and take
their turn.

We are very certain in the Federal
Defenders Office that you shouldn't look at
taking these submersibles and simply join them
into what is done with the Go Fast Boats, and
there's five very good reasons. The first one
is that in the Go Fast prosecutions, which is
under the drug guideline, they have drugs.
In fact, we've been getting semi-submersibles,
as well as Go Fast Boats, with drugs on them,
and they've been prosecuted under the drug
statute for years.

If there's drugs, that's where
it's prosecuted, and that's appropriate.

In the semi-submersibles, that was
designed to catch the ones where there aren't
drugs. Either they don't have a load, they've
dropped it off. Theoretically, it could be
used for something else. At this time, we
don't know of any other use.

When we look at some of the other
things that make sense and that go into the
drug statute, there are three types of crimes
now I can identify where it's clear that drugs
are involved but you don't have drugs. Let me
start with paraphernalia. As opposed to
having the drugs, we know it's related to
drugs. We know it's indicative of drug use,
but we don't have it. We have the same thing
when we get into the tunnels, and the tunnels,
I think, are most closely analogous.

We know we have drug trafficking
doing this, but if we don't catch the
smugglers at least we can prosecute the
tunnels. And we have the same thing going on
here. If you catch the submersible and don't
get any drugs, at least you have the
submersible because, at this point, we believe
that's what it's involved in.

Now, in those situations what do
we see as the sentencing policy that has been
followed, which is that we have a much lower
sentencing range. I see my time is almost up.
If I could finish this? We have a much lower
sentencing range. You have in the
paraphernalia, instead of drugs it can be a
base offense up to 38, we have paraphernalia
at a base offense of 12. The smuggling of
drugs 38, but tunnels is 16. The Go Fast
Boats or the submersibles with the drugs 38.
We propose the appropriate base offense level
It is lower than what we would see on the tunnels for several reasons. The tunnels, in that case what was important was the government prosecutes the organizers, the builders, the financiers. They use more involved construction, and they're, in fact, harder to find. While tunnels deliver their goods directly into the American public, the Go Fast Boats aren't coming to America and neither are the submersibles. While there has been some instances of Go Fast, none of the submersibles have been found within American waters and, in fact, they're going usually to Central America. Many sink, many are pirated. And then the drugs themselves go from Central America throughout the world. They don't deliver directly. Moreover, the drug guidelines 2(b)1.1 are based on having amounts of drugs, which we don't have here, and offer opportunities to reduce things, which we wouldn't have with the submersibles, the safety valve, the minor role, and things like
that.

I was going to address the congressional directive, but my time is past. If you want to speak with me about that, I'd assume that would be good.

It's a directive to consider, and many directives to consider are overlooked [and] are not enacted because there are already scant guidelines that cover it. And that applies to most of these, and that was in my written testimony as to what things could apply.

I do want to note that the one thing that's important here, though, is, as to organized crime, the idea of bumping it up for being an organized crime. We know with the complex tunnels, with the Go Fast, and with the submersibles at this time that they are being used by organized crime to move drugs. That is inherent in why it's being criminalized. So all of them, when you don't distinguish between two different types of people, there's no point in bumping one up if
all cases are going to be there.

We have the other thing which is that -- I lost my thought. If you enhance with organized crime, right now we don't have in the tunnels cases a minor role sort of thing, and we have not had it in the boat cases, as well.

Let me tell you about why my district and, in particular, my Tampa in my district is where all of the boat cases are brought by the Department of Justice. There may be some logical reasons to bring them from the Pacific into us and from other parts of the world, but we do know that in my district and in the 11th Circuit the law is, and it is being followed religiously with only the very occasional exception, no minor role will be given. The judges will treat it as we look only at what's on the boat and what people are doing on the boat, not the entire criminal organization. And, therefore, since everyone is taking turns driving the boat, they're all equal. We have no minor role.
If there was to be an organized crime addition, we really have to make sure we make clear that then we have to consider all that and minor role has to be in there. And if I could add one further thing, from the defenders in Tampa, we would ask the Commission to consider revisiting 2(d)1.1 minor role and in the comments adding some real teeth to the fact that those things ought to be considered in the role of the entire thing so that we may not have the monopoly in the future on the boat cases. And I thank you so much for the extra time.

ACTING CHAIR HINOJOSA: Thank you, Ms. Elm. Mr. Linn?

MR. LINN: Chairman Hinojosa, Commissioners, good evening and Happy St. Patrick's Day. On a day traditionally spent consuming green beer, it appears the Commission is fully functional.

The United States Sentencing Commission was instrumental in the length of stay changes that were codified for those
sentenced for criminal activity that occurred after November 1st, 1987. The result of the elimination of parole and old law good time and the de facto doubling of sentences has led to the tripling of the federal inmate population in little over 21 ½ years at a cost of nearly a trillion dollars to the nation's taxpayers for prisons, courts, prosecutions, defense, and post-incarceration supervision. The Federal Bureau of Prisons is now operating at 137 percent of capacity with over 203,000 inmates. The BOP is now resorting to triple bunking in cells designed for one inmate because of the ramped overcrowding, and there are stabbings and riots almost on a weekly or bi-weekly basis. The federal prison system is made up primarily of low-level drug dealers with sentences that sometimes exceed that of murderers and rapists at a cost of a minimum of $40,000 per inmate per year.

What looked like a good idea when the Sentencing Reform Act of 1984 was conceived has instead been an abject failure.
It was disavowed many years ago by its primary author Eric Sterling and many of those in the criminal justice community have been calling for change to the dismal consequences of an overly harsh system of punishment that costs more than the country can afford and extends the length of stay for nearly all inmates to an unjustified extreme.

Last summer, FedCURE was privileged to be invited to a symposium put on by this Commission. This symposium's title was a welcome breath of fresh air, "Symposium on Alternatives to Incarceration." At that conference, speaker after speaker presented treatises documenting evidence-proven ways to deal with those already incarcerated, including expanding good time, re-institution of parole, and alternative plans to recidivism for technical violations, all to reduce the prison populations.

At the root of all recommendations centering on reducing the prison population is a conclusion that our current form and range
of punishments are disproportionate to the harm that has been inflicted. Moreover, current efforts to punish those who commit such crimes are not cost effective.

It was obvious to me long ago that the states are way ahead of the feds in this regard except for one small branch of the DOJ. The National Institute of Corrections has an ongoing endeavor called the Norval Morris Project. It's calling for the halving of the present population in federal prisons and the halving of the federal post-incarceration populace, as well. A paper by James Austin explains hows and the whys and the wherefores far better than I can, but rest assured that this approach to alternatives to incarceration and FedCURE's focus are one in the same.

The good news is that the necessary reforms have either currently been adopted in many states or were in use previously, so the desired reduction is readily achievable. It should also be noted that changes are neither radical nor need to
take a long time to implement. What is required is relatively modest but steady changes in current practices over a sustained period of time. This is because relatively small adjustments in key decision points will have a large cumulative effect over a relatively short period of time.

Recently, the Pew Center on the States has argued that new supervision strategies and technologies can help manage more lower risk offenders safely outside of prison at lower cost and with better results than incarceration. Such efforts needs to be strengthened, not scaled back at a time of budget crisis, said Pew.

With all of these thoughts in mind, FedCURE presented its suggestions to the Commission for inclusion in their next cycle of recommendations to Congress. Our recommendations were not adopted. Apparently, there's a difference of opinion as to whether the Commission may have the statutory authority to make the dramatic changes that
are necessary to solve the present problem of "length of stay."

Specifically, the Commission's proposed recommendations to Congress for May 2009, as they are presently specified, do not in any way attack the back end of sentences already set.

At this time, 1(b)113 of the guidelines manual gives authority to the Director of the BOP by its motion to seek release of any inmate if the court finds extraordinary and compelling reasons warrant the reduction. FedCURE requested the manual give authority to give that same director the ability to inclusively seek earlier release by a speed up of good time and an authority for the Chairman of the United States Parole Commission to give a second look to long-term inmates who might be parolable under their guidelines.

Admittedly, it's not an exact comparison to match 1(b)113 with our proposed 1(b)114 and 1(b)115, but the Commission has
only two options here. It can either continue down its present path and let the BOP attempt to build its way out of this incarceration crisis and hope that Congress decides to appropriate hundreds of billions of dollars to undertake this foolish course of action; or it can take a bold initiative and interpret broadly so as to recognize very "extraordinary circumstances" here that are included in the statutory construction of 18 USC 3582(c)(1)(A).

The question here is one of interpretation of the statute and a decision as to what are extraordinary circumstances. In short, it is the position of FedCURE that it is unlikely this government or this Commission will face anything more extraordinary in order to justify the intervention that is surely necessary. It is all a matter of interpretation.

This is the reason why FedCURE requested our presence on your agenda today. We argue that the Commission has a unique
opportunity to do more than make minor sentencing guideline changes for future federal inmates. FedCURE feels that the Commission was given a mandate by Congress to make wholesale changes to the criminal justice system when it deemed that extraordinary circumstances demanded change. That is exactly what FedCURE requests be done today for the Commission’s next recommendations to Congress.

At the very least, if the Commission feels their present mandate does not include the steps necessary to attack the back end of sentences, as well as the front end, then we strenuously request that you go to Congress and resolutely insist that such authority be recognized and not let years go by while this situation worsens.

Thank you for the opportunity to make this presentation. My name is Kenny Linn. I am the Chairman of FedCURE. FedCURE stands for Citizens United for the Rehabilitation of Errants. We represent over
203,000 federal inmates and somewhere close to a million of their family and loved ones.

Thank you again.

ACTING CHAIR HINOJOSA: Thank you, Mr. Linn. Are there any questions?

COMMISSIONER CARR: Yes, I have a question. Is your understanding of these semi-submersibles consistent with what I think we've been told by the Coast Guard, which is that they frequently cost about a million dollars each to build?

MS. ELM: Let me also say I have brought with me the lawyer who's assigned to our first submersible case under this. Adam Tanenbaum is here in case you want to direct it to him.

My understanding is that it's not quite as much, that some of them are going upward of a million but others are lower, closer to $500,000. They are somewhat substantial, and, of course, the people who are on it can't bankroll that.

COMMISSIONER CARR: But it does
suggest that they're being used for an expensive shipment of something?

MS. ELM: Yes, as are those fancy tunnels and paraphernalia.

VICE CHAIR SESSIONS: Your comments about use of the minor role reduction in Tampa are interesting because when we were in Atlanta just a short while ago we were told that there is somewhat of a split among the judges in Tampa as to whether or not they apply minor role adjustments in cases like what you suggest. It wasn't necessarily related specifically to submersibles, but, generally speaking, there is at least one judge, if not more than one judge, who does apply minor role adjustments; is that not right?

MS. ELM: Here's my understanding that we do have one judge who I believe addressed you in Atlanta who has given minor role some of the times, that this is --

VICE CHAIR SESSIONS: So that was the one judge who admitted to using minor role
adjustments in cases --

MS. ELM: And my understanding [is that] he has done that. We had one other judge I heard about in the last just little while gave one minor role. So it may be that we have sort of a loosening coming up, but it still is very entrenched, and a number of our judges are lockstep on this idea. We're very concerned about that because, as a result, we're flooded with the boat cases.

ACTING CHAIR HINOJOSA: Are there any other questions? If not, thank you all very much. We certainly appreciate you waiting all afternoon. I do want to also, on behalf of the Commission, note that Harriett Galvin who is in the audience here is spending her last day with us as the Assistant U.S. Attorney who has done a stint here at the Commission, and we thank her for her work. She's from the Southern District of Florida. She has received a lot of compliments from the staff, and the Commission appreciates very much her work here.
We also have Molly Roth who is present who is the Assistant Federal Public Defender, but she'll be here through May probably, and she's from the Western District of Texas. And so we thank both of them very much for their service and look forward to continued input from them through the coming years. Thank you all very much.

(Whereupon, the above-entitled matter went off the record at 5:47 p.m. on March 17, 2009 and resumed at 8:38 a.m. on March 18, 2009.)

ACTING CHAIR HINOJOSA: Good morning. This morning represents a continuation of our public hearing with regards to the new guidelines and amendments the Sentencing Commission is considering for this amendment cycle. We have a distinguished panel of five individuals who will be addressing the Court Security Improvement Act of 2007 and share their thoughts with regards to what the Commission has published for comment.
We have Mr. Michael J. Prout who is the Assistant Director for Judicial Security in the Judicial Security Division of the U.S. Marshals Service. Mr. Prout is the principal advisor to the Director and Deputy Director on all matters of personal, technical, and physical security of the federal judiciary.

We also have someone who we all know, Jon Sands, who is the Federal Defender for the District of Arizona. As we all know, he is the Chair of the Federal Defender Guidelines Committee and has served as special counsel to the Commission. He is a newfound fan of the University of Texas basketball team.

We also have Mr. Todd Bussert who is a criminal defense attorney in New Haven, Connecticut. He is the former Associate Director of Client Services for the National Center on Institutions and Alternatives. He is currently the co-chair of the Commission's Practitioners Advisory Group which provides
invaluable advice to the Commission.

We also have Mr. Eric R. Stegman who currently manages the Communities of Practice Program and assists with communication strategy for the National Congress of American Indians Policy Research Center. He has assisted in the development of the tribal criminal law and procedure textbooks.

We also have Dr. Mario Scalora, who is an Associate Professor of Psychology with the Clinical Training and Law Psychology Program at the University of Nebraska at Lincoln where he conducts and supervises research on various aspects of targeted violence. He also currently serves as a consultant to the threat assessment unit of the U.S. Capitol Police.

Each one of them brings great experience to the subject, and we look forward to hearing their statements. We will start with Mr. Prout. The rules are seven minutes for each individual and then obviously
questions and answers from the Commissioners.

There is a lighting system up there that gives you a two-minute warning when it turns yellow.

If you're like me, you try to run the yellow light, but when it turns red apparently the time is up. So we'll start with Mr. Prout.

MR. PROUT: Chairman Hinojosa,
distinguished members of the Commission, thank you for allowing me the opportunity to testify on behalf of the U.S. Marshals Service. Today I will address the issue of violations of 18 USC Section 115 and 119 that occur through the use of the internet, as requested in Section 209 of the Court Security Improvement Act of 2007.

The Marshals Service views inappropriate communications and threats made via internet postings and blogs very differently than those through other delivery methods. Unlike a letter or an e-mail, comments posted on an internet website have the potential to be viewed by a countless number of persons. Internet postings that are
hypercritical and contain restricted personal information of a protectee, such as their home address or Social Security number, can create a large number of potential threateners virtually unknown to the Service. Such a scenario can be extremely difficult to accurately assess and can, therefore, lead to the expenditure of an extraordinary amount of resources to ensure the safety of our protectees.

Internet threats should also be differentiated from other types of public forum events, such as radio, television, or a speech made in a public setting. While these forums can also reach a large unknown audience, they're different in that they only generally reach the audience that happens to be listening or viewing them at that particular moment, and they're done in a public forum, which can easily become known to law enforcement. The audience to an internet threat can be multiplied exponentially, and the blog or website may be completely unknown.
To guard against violating a person's First Amendment rights to free speech, the Marshals Service requires the occurrence of a triggering event before a protective investigation is initiated. In the area of threat management, a triggering event is the receipt of inappropriate communication or a reasonable indication that a possible threat exists.

However, one of the issues that makes internet threats so insidious is that others who hear or read this free speech may interpret it differently. They may interpret it as a call to violence or a threat of violence and be influenced to act out accordingly. If the threat on the internet is also accompanied by restricted personal information, it can assist in facilitating the act of violence by identifying the location of the protectee.

In the last five years, inappropriate communications to Marshals
Service protectees increased 89 percent.
Threats received via the internet, while
amounting to between 1 and 2 percent of the
total, have followed this trend. Going back
to 2006, inappropriate communications received
via the internet versus all inappropriate
communications received were as follows: in
2006, 12 internet cases from a total of 1,111
cases open; in 2007, 13 internet cases from a
total of 1,145 cases; in 2008, 15 internet
cases from a total of 1,278 cases; and in 2009
to date, 8 internet cases from a total of 478
new cases.

In the vast majority of these
internet cases, the threat or inappropriate
communication was directed at a single case-
specific victim, usually the presiding judge
in a particular case. In rare cases, the
threat made references to more than one judge
or to a prosecutor, case agent, or family
member. Internet cases do not necessarily
create volumes of victims. They do, however,
create volumes of potential threateners.
I'd like to share with you a few examples of recent cases involving threats over the internet. In February 2009, a federal judge heard a civil case where an illegal alien sued a U.S. citizen for violating their civil rights by detaining them as they illegally entered the United States through his property. The judge rejected a motion to dismiss the case, and the case proceeded to trial. One individual posted the judge's home address on a blog, while a radio talk show host announced the judge's chamber's phone number. Many others responded with comments on the blog that were threatening, stating that the judge should be hung, shot, or visited with other violent acts. The judge received hundreds of phone calls to his chambers, many of which were threatening and inappropriate. As a result, a protective detail was established on the judge until the trial was completed and the public furor receded.

In June 2008, a white supremacist
radio talk show host released the home addresses, telephone numbers, and work addresses of two federal judges on his radio broadcast and the show's website because he did not like decisions they made pertaining to immigration. He announced to his audience that both judges were traitors to the United States. He called for citizens to visit the judges at home away from the protection of the Marshals Service. He suggested face-to-face confrontation as a method for airing discontent with the rulings. He stated that he can picture himself punching out these judges, kicking them in the rib cage and the head, and then challenging them on their decisions while they lay on the ground. He remarked that he would have a really good time beating the judges and suggested that his listeners would enjoy the activity, as well.

Clearly, his intention was not to actually perform these acts himself but to incite others to attack the judges. The radio host's comments resulted in the establishment
of protective details on both judges until the
host, after being interviewed by the Marshals
Service, retracted his comments on the air and
on the internet.

Ed and Elaine Brown are members of
the United States Constitution Rangers, an
anti-tax, anti-government organization
originally established in Arizona in 1977. In
January of 2007, the Browns were both
convicted in absentia after they stopped
attending their trial. They retreated to
their compound and refused to surrender to the
Marshals Service, creating a standoff which
lasted for seven months.

During this time, the Browns
themselves made no threats to any judicial or
law enforcement official other than to
proclaim their intention to defend themselves
with violence. However, one of their
supporters posted a letter on the internet
stating that the judge, U.S. attorney, and
various other officials should be hanged for
treason. This post initiated a long internet
campaign of threats and inappropriate communications directed at Marshals Service protectees from the Brown supporters and other anti-tax and anti-government groups, and the activity resulted in protective details on several judges and prosecutors for months.

Of tremendous concern to the judiciary and others the Marshals Service protects is the proliferation of personal information on the internet. Our knowledge of the planning of attacks on the judiciary shows that approaching a protectee at their residence is an advanced stage of planning. A history of attacks against a judiciary has shown that successful attacks all took place at the judicial officer's residence. 18 USC 119, protection of individuals performing certain official duties, makes it illegal to intentionally release personal restricted information with the intent to threaten, intimidate, harm, or incite the commission of a crime of violence to a covered person.

The Marshals Service is greatly
concerned about the use of the internet to threaten and intimidate its protectees and appreciates the opportunity to address the Commission on this topic. The consideration to increase penalties for violations such as these is a valuable tool for the challenge faced by the Marshals Service in its protection of the judiciary.

That concludes my prepared remarks. Let me say again how much I appreciate the Commission's time and attention of these important issues.

ACTING CHAIR HINOJOSA: Thank you very much. Mr. Sands?

MR. SANDS: Judge Hinojosa and members of the Commission, I'm honored to be here yet again to discuss the sentencing guidelines and the request of the Commission that the federal defenders and community organizations give their views.

I have worked over 20 years with the guidelines, 15 years before the Commission, and 10 years as Chair of the
In these times, we have appeared in front of 
you urging the Commission to study and to look 
at what the Commission is doing.  

Almost four years ago to the day 
when the Commission voted to increase 
penalties for homicide and assault 
convictions, Judge Sessions stated his concern 
that in passing judgment based on numbers the 
Commission looks to individual enhancements 
that might require an increase. He noted that 
no body seems to consider the big picture or 
the cumulative effect of all the little 
decisions that the Commission makes. He 
further noted that, as a result, the penalties 
seem to continually grow based on apparently 
legitimate reasons. If one looks at the 
overall system, which is not known to be 
particularly lenient, it is continuously 
becoming more severe. 

Recognizing that penalties 
constantly get ratcheted up with the 
interaction between legislation and the
Commission's concern with proportionality,
Judge Sessions speaking at the hearing
emphasized that the Commission's duty is to
make independent judgments and that it is to
reflect upon the ultimate goal of 994 and
3553. We would urge the Commission to adopt
this as a guiding star in looking at this act
and in future acts. What is the purpose of
punishment? What is the Commission doing?
How is it affecting 3553 and 994?

Sentencing is more than just
raising two levels or four levels or putting
in comments. Is the sentencing addressing
what is meant as punishment? And this is more
coming before the Commission with anecdotes
about this case or that case. We all
recognize the terrible price that crime takes
the victims. But at the end of the day, what
are we doing? What are judges doing?

The Commission is in an important
place right now as an expert body. It has
developed the expertise and now has over 20
years of experience in sentencing and
empirical data to look at what sentences should be and where they are going. Thus, the Commission, using its expertise, should look at the dialogue that the judges have with the Commission through actual sentences. What is being done in particular cases? What do trends show? What do social scientists report in their studies? In this way, the Commission, in looking at whether to increase sentences or decrease sentences, has the best ability and the best knowledge to act.

Frequently, law enforcement comes in front of the Commission saying we need to increase this, we need to increase that. It's the crime of the day, the crime of the month. But the Commission has to step back and say where is this all going? Nowhere is this more apparent than in those offenses that affect Indians. And in the raising of the statutory maximum for homicide and for assault, there's a very real risk that the Commission in acting could affect defendants that are over-represented by Native Americans.
Native Americans make up one percent of defendants, yet they are over-represented in violent crimes. The over-representation is due to the fact of the special relationship between federal jurisdiction and the Indian tribes. Federal jurisdiction on many reservations is the only law enforcement. And as a result, many offenses that would be treated in the state jurisdiction or common law is brought into federal court. As a result, Native Americans feel the brunt of offenses that Congress or others might not have thought would affect them.

In assault cases or homicides, this is not a case of extortion, this is not a case of organized crime, this is not a case of violent bank robberies. It's frequently brother against brother, cousin against cousin. There's alcohol abuse. There's poverty. All of these things weigh against the Commission acting without further study. And toward this, we would urge the Commission
to take advantage the way it has in the past and form an ad hoc Indian study group. It was done several years ago. This would bring the stakeholders to one table: judges, prosecutors, defense counsel, community organizers, and members of the tribe to discuss what is best for those offenses that affect Indians. An ad hoc study group for Native American crimes was successful. It brought to the Commission recommendations based on research and on empirical data, and the Commission acted on several of them.

We would urge the Commission in reviewing crimes that affect Native Americans to take that path and to look at the special study groups for other offenses, as well.

Thank you.

ACTING CHAIR HINOJOSA: Thank you, Mr. Sands. Mr. Bussert?

MR. BUSSERT: Judge Hinojosa and members of the Commission, my name is Todd Bussert. I'm from a private practice in New Haven, Connecticut. I've been invited here
today to testify in my capacity as the Vice Chair of the Practitioners Advisory Group on behalf of Chair David Dubold of Gibson, Dunn & Crutcher here in Washington and other members of this steering advisory group. It's always a pleasure to be invited to share our views on proposed Commission actions. What follows are our group's views concerning proposed court security amendments upon which we'll elaborate further in our written comments to this and other proposed amendments before the end of this public comment period.

As part of the Court Security Act of 2007, Congress increased the maximum statutory penalties for several offenses. The Commission has asked whether the current guidelines are adequate. The PAG believes that they are and that increases in applicable base offense levels are unnecessary.

Congress began work on what eventually became this act in 2005. At that time, bills were introduced in both chambers that carried mandatory minimum penalties for
most of these offenses, penalties that were
removed ultimately during the legislative
process. PAG believes that with Congress'
rejection of statutory mandatory minimums,
coupled with an absence of any directive to
increase guideline penalties, the Commission
should not assume that the increase in maximum
penalties signals a need for higher guideline.

The PAG is particularly concerned
about an increase in base offense levels that
would affect typical offenders in the name of
punishing what are perhaps best characterized
as the most egregious of cases. As the
Commission is well aware, the guidelines are
attended to address the heart of criminal
misconduct for defense categories such as
these that has accomplished the establishment
of base offense levels suitable to punish the
typical low-end offenders in appropriate
enhancements. When base offense levels are
shifted upward simply because Congress has
increased maximum allowable penalties for the
most serious offenses and offenders, the
result is too often the ratcheting up of guideline penalties that has been the subject of so much criticism for the past two decades.

Viewed objectively, that is absent a political prosecutorial prism, the guidelines for these offenses that this Commission has already considered and promulgated are adequate and do not require changes to accommodate or account for new statutory maximums. The Act raises the penalty for assaults resulting in serious bodily injury or involving the use of dangerous weapons from 20 to 30 years and for assaults involving physical contact or intent to commit another felony from 8 to 10 years. Sentence calculations for these offenses are referred to Guideline Section 2(a)2.2.

In 2007, the mean sentence for non-sexual assault over all criminal history categories was 39 months and the median was 30 months. Even criminal history category 6 offenders received sentences at multiples below the former 20-year maximum,
approximately 6.3 years on average. Such empirical evidence counsels strongly against any need to increase guideline ranges. Indeed, of the 313 sentences for assaults in 2007, fewer than 6 percent were above the guideline range, while approximately 12 percent were non-government sponsored sentences below the range.

Importantly, Section 2(a)2.2 already recommends ranges at or approaching the new statutory maximum for those who engage in the most serious of conduct, especially where the victim is a judicial or federal official. For instance, a base offense level of 14 with enhancements for conviction under Section 115, more than minimal planning, discharge of a firearm, serious bodily injury, payment, and an official victim results in an adjusted offense level of 36. This produces a range of 188 to 235 months for first offenders in ranges that exceed the statutory maximum for those in criminal history category 5 or 6. In other words, the guidelines as
currently written produce guideline ranges at the statutory maximum. To the extent the guideline range in a given case is not sufficient to satisfy the purposes of sentencing, courts remain free to depart upward or impose a non-guideline sentence.

The statutory maximum for voluntary manslaughter is also increased from 10 to 15 years. Under the current Section 2(a)1.3, the base offense level for such a conviction is 29, which increases to 35 when there's an official victim. Without any other adjustments, for a category 1 offender, this results in a range of 160 to 210 months. That is a range that exceeds the new statutory maximum. Accordingly, no further changes are needed. In this regard, the PAG notes that the Commission raised the base offense level from 25 to 29 less than five years ago, and there's no empirical evidence that establishes or suggests that courts find level 29 insufficient.

Turning attention to official
victims, the Commission has requested comment on whether Guideline Section 3(a)1.2 addresses adequately the circumstances of an official victim. The PAG believes that it does. In 2004, the Commission increased this adjustment from three to six levels for offenses against a person motivated by the official status of the victim. In all other circumstances, it is a three-level enhancement; and, as an appropriate point of comparison, Guideline Section 3(a)1.1 provides a two-level enhancement for vulnerable victims.

As touched upon during our testimony last March, the PAG believes that any further increase based solely on the victim's status suggests, if not actually establishes, a class system within the guidelines where in the harm that may befall judges, prosecutors, probation officers, and other federal officials is treated far more serious than that visited upon the average citizen, that their lives and property are somehow more worthy of protection. An example
helps illustrate this disparate treatment.
Say you have a former assistant United States
attorney who, having seen the light, is now
toiling diligently as defense counsel. Six
months after entering private practice, this
capable young attorney has a client who,
following sentencing, becomes disenchanted not
only with the system but also with her,
notwithstanding the consensus of view that she
did a terrific job securing a favorable
disposition of her client.

Disgruntled client, who's been
permitted to surrender voluntarily, decides to
exact revenge before entering federal custody
by committing an offense of which counsel is
the victim. Under the current system, there's
no status-based enhancement for this former
prosecutor, nor should there be. But as
things already stand, there would be at least
a three-level and as much as a six-level
enhancement if the defendant's resentment had
instead been directed towards someone
maintaining an official court or other
government position.

This difference in penalties is sufficient to address the status issue and congressional concern. There is no justification to magnify it further. Indeed, we have not heard or seen anything in the past four years to suggest that courts are dissatisfied with the level of added punishment called for under Section 3(a). It is a particularly sensitive matter and unavoidably so for a government agency to establish the appropriate sanctions for making a government employee or victim of criminal conduct. Prudence demands that any greater differentiation and punishment due to official status be based on credible documented evidence tied directly to the need to be addressed.

Finally, Section 209 of the Act, which directs the Commission to review threats that occur over the internet in violation of 18 USC Section 115 to determine whether and how much the circumstances should aggravate
the punishment, the PAG notes that this language only requires a review, not a change, and no change appears necessary. Using this offense characteristic to enhance the base offense level for defendants who threaten a current or former federal official or her family member is irrational, both logically and factually.

Threats can be conveyed in any number of ways. Among the most common would seem to be in person, that is face to face, by phone, by mail, and over the internet. Of course, over the internet can have any number of meanings, such as via e-mail, in a social exchange group like Facebook, in the comments section of a blog, or on one's personal website, just to name a few. Yet, the most aggravated of these is the in-person threat in terms of its intrusiveness, imminence, and opportunity for escalation. Likewise, anyone who has received a harassing phone call in the middle of the night can attest to how disruptive and disconcerting it can be. And
receipt of a letter informs the recipient that the individual who made the threat knows where he lives.

There are numerous difficulties in seeking distinguished internet threats from these types of threats. First, it can be reasonably argued that someone who goes through the deliberate steps of writing a letter, addressing an envelope, applying a stamp, and placing the letter in the mail is more determined to communicate a threat than someone who types out an e-mail and clicks send. It's fair to say that all of us either have written e-mails in the heat of the moment that we later regret or have surely seen our share of such e-mails on our office exchanges or listservs. A form of communication that engenders immediate, sometimes detached or presumably anonymous responses does not, in and of itself, require an added level of punishment. To the contrary, it would seem to compel a degree of understanding as to the stressors that we're acting upon the
individual.

The second problem is perhaps probably relatable to generation gap. Notwithstanding what has become the omnipresent existence of electronic communication in our society, there continues to be a lag between the understanding and appreciation for what computers, cell phones, and the like mean to those aged 35 and younger, as compared to the rest of us. It is seen in areas ranging from the willingness to abandon privacy by living openly via Facebook to the demise of newspapers because young people can find information freely available online.

In other words, for a growing number of Americans, electronic means of communication are simply the norm. Without more, this fundamental change in the way we communicate is clearly not aggravating relative to criminal misconduct.

In the same vein, it is notable that, while the internet fosters an apparent
sense of anonymity among many, the reality is
that the use of electronic means to
communicate make it easier for investigators
to identify and locate someone, certainly
easier than identifying the sender of a letter
with no return address. And, again, without
more, someone who attempts to conceal from
where an internet threat originates should be
treated no more severely than someone who does
the same using other forms of communication.
There is no legitimate basis to distinguish
one group of individuals from the other.

If anything, by increasing
punishment for those who use the internet to
convey threats, the Commission would reward
the use of other forms of communication with
greater risks. A clear example of this is the
number of anthrax-related safety precautions
taken in mail rooms throughout the country

The PAG believes that creating an
aggravating factor for the use of the internet
will cause courts to disregard the guidelines
for reasons like those for which they have increasingly rejected to congressionally influence child pornography and drug guidelines. The PAG, therefore, urges the Commission to take no action in this regard. Thank you.

ACTING CHAIR HINOJOSA: Thank you, Mr. Bussert. Mr. Stegman?

MR. STEGMAN: Good morning, Chairman Hinojosa and the distinguished members of the Commission. Thank you for giving me an opportunity to discuss the proposed changes with you this morning. As an initial note, I would just like to say that I'm not testifying to you in my official capacity today as an employee of the National Congress of American Indians and that my statements do not necessarily represent views of NCAI.

There are three proposed amendments in the 2009 proposed amendments to the sentencing guidelines that will have significant impacts on Indian country: one,
the provisions governing an increase in the maximum sentence for involuntarily manslaughter from six to eight years under the Court Security Improvement Act, which would affect sentencing in Indian country DUI cases; two, the provisions governing increases in the maximum sentences for witness/victim tampering and retaliation, which would have significant impact in Indian country domestic violence and child abuse cases; and, three, the provisions governing an increase in the maximum sentence for influencing, impeding, and retaliating against federal officials, which would effect conduct against BIA officers.

I've spent the last three years as a researcher on a forthcoming National Institute of Justice study on the administration of justice in Indian country, and one thing that's become very clear working on that project and that's the disproportionate relationship that tribal citizens have with the federal system. Indian tribes have a very unique relationship with
the federal government, as you know, especially as it relates to criminal jurisdiction. Where most Americans typically encounter the state system for crimes under review today, tribal citizens are much more frequently prosecuted under federal law and, in many cases, being served by federal police and probation officers. It is this frequency and day-to-day relationship with the federal system that warrants careful review of these proposed guideline changes because they disproportionately affect Indian country.

We were able to review the work of the Native American Advisory Group in 2003 that Mr. Sands referenced and the 2003 testimony of Paul Charlton before this Commission. The conclusions of the Advisory Group and the testimony of Mr. Charlton bring out two persisting concerns: one, a concern that Native American defendants are treated more harshly by the federal sentencing system than they would be if they were prosecuted in their respective states; and, two, that in
states with higher sentences than in the federal system the perception that real injustice is suffered by many Indian and non-Indian victims where the defendant gets a much lower sentence than if he or she were prosecuted under the state system.

While we were able to contact and speak with the U.S. attorney and victims advocates in Arizona where they conveyed full support for these proposed amendments on behalf of their victim population, we feel that it is important to have more time to contact and get feedback from the following: the U.S. attorneys and victims advocates in other states with large native populations; tribal prosecutors and public defenders; tribal domestic violence and child welfare programs; the native MADD chapters, Mothers Against Drunk Driving; the native victim advisory groups; and the legal academic community working on Indian country issues; and, finally, native legal aid organizations.

The Indian country entities that
we were able to contact report that they would like more time to analyze the proposed amendments and comparative laws and to review available statistics and new information. We understand that the notice and comment period remain open until March 30th. However, we also expect that it may be necessary to take consideration of these amendments into our next cycle.

Presently, there are two members of the Victim Advisory Commission, one whom I'm speaking on behalf of today, Pat Sekaquaptewa, and the other, Monte Deer, who have committed to following up with these entities and seeking out more input. Thank you very much for your time.

ACTING CHAIR HINOJOSA: Thank you, Mr. Stegman. Dr. Scalora?

DR. SCALORA: Thank you. Distinguished members of the Commission, I'm Mario Scalora. I'm an Associate Professor of Psychology at the University of Nebraska Lincoln, and I have the privilege as serving
as the consulting psychologist at a threat
assessment section of the U.S. Capitol Police.
I should state as a caveat up front that I am
not representing neither the University, nor
the United States Congress, nor the U.S.
Capitol Police. However, I can speak with
great certainty that many of the agencies I
work with are very much strongly in support of
any activity that would enhance the safety of
judicial officials and those who work with the
courts. I will not read my testimony to you
because I tend not to read out loud as well as
I speak out bullet points, but I do not mean
that to presume any informality, only respect
to the Commission.

I had the opportunity over the
last 15 years of looking at literally tens of
thousands of threats to government officials
at the state and local level. Many of the
individuals at the Capitol Police deal with,
I would say a minority, but easily 20 percent
overlap with the Judicial Branch. We
unfortunately share some of those individuals
who are gifted in expressing their grievances toward government officials. And there tend to be some commonalities but also some aspects of this that are evolving. One, we know that threats toward any government official can not only be rather taxing toward the official and his or her family but also to the agencies that have to spend a great deal of effort, as Marshal Prout described in a few cases earlier, in terms of the amount of energy it takes to maintain and address and manage those threats.

That being said, I would caution that any focus on the use of the internet as justification for enhancement be viewed almost like a double-edge sword. In one respect, we know that electronic communications have exploded toward government agencies and, as a result, the small numbers of those that cross First Amendment protections into the realm for vague or direct threats continue to grow. We know, for example, as stated by one of my colleagues here, that many of these activities
are done by younger people. Frankly, they
type better with their thumbs. Two, they're
much more savvy about these issues. But even
with that, we do find that even folks of our
age group are still becoming more and more
internet savvy, but there is a
disproportionality related to age.

We also know that, for example, a
few years ago [inaudible] published a study
comparing e-mail and letter threats. We
consider these very different. We know that
e-mail threats tend to be much more impulsive
and, by themselves, tend not to result in a
direct action of harm toward a member. That
does not mean that we do not take every threat
seriously, and in some cases part of the
mitigation may be the result of the actions by
the agencies. Threat cases are very easy to
manage, frankly, because federal officials and
state officials have a few more tools at their
disposal to address the individual who uttered
the threat. But our experience has been that
it's very easy and I'm relieved to know it's
not just professors and students but people
across the gamut can sometimes hit send
prematurely.

We also recognize, as pointed out
earlier, that there are a range of
communications that people express
electronically: response to news stories,
blogs, social networking sites, Twitter,
basically messaging services. Many of these
things can be very impulsively done, but they
can also be used as part of a campaign of
harassment where personal information
regarding the individual at focus could be put
out there at risk to that public official.

For our purposes with the Capitol
Police, we do not focus on a single modality.
We focus on a campaign of harassment or a
campaign of intimidation for that person, and
we find very often many of those people cross
modalities of contact. For example, we have
found people doing rap videos on Youtube, and
some of those rap videos, not all of them by
any means but some of them have been very
threatening in nature. Those, by their very nature, have not necessarily gone forward to threatening activity, but individuals who've posted Youtube entries have then gone on to blogs, then posted e-mails, sent letters, made phone calls. We have found ourselves to be much more concerned about those individuals because they display what we describe as an intensity of effort. And, frankly, those are the people we worry about.

And I would also caution that if one is going to focus on the modality of how threats are delivered, you're going to always be behind the technology. Four or five years ago, we were just trying to figure out e-mails as they exploded after anthrax showed up at Capitol Hill and other government buildings and trying to figure out how to review those. We are now dealing with the range of electronic communications now and trying to get our arms around all of those things, and the sophistication and the variety at which those are coming to us continues to evolve.
And so if you are going to look at this, I recommend you use a broad definition but focus more on the nature of the behavior versus the modality.

Second, there was some consideration of whether the sender of threats is acting on an individual capacity or is part of a large group. I can appreciate why members would be concerned about that and why Congress might encourage that type of scrutiny. As the Marshal described earlier, there are specific groups that, frankly, have become much more active in recent years with regard to these activities.

We've noticed, though, some changes in how these groups behave. These groups have become much more decentralized and, frankly, don't hold a lot of meetings anymore. They use the internet as a recruitment tool and a tool to incite members; and, frankly, one could have an infinity for a group, may never have, quote, "formal membership," but can be encouraged and
educated by a group through a variety of electronic means and being able to, quote, "tie" that person to a group can be extremely difficult. And I think we see this with transnational threat groups, as well as very specific issue-oriented or domestic threat groups. And if the Commission believes this to be an important distinction, fine. I would not hold my breath, with all due respect, that you're going to get a lot here in that regard.

When I do training with front-line officers, and I'll stop here, we do not ask people for their al Qaida membership cards when they show up on Capitol Hill. Membership is a rather ubiquitous issue with many of these groups. Thank you again for the opportunity.

ACTING CHAIR HINOJOSA: Thank you, Doctor. I'll open it up for questions.

Commissioner Carr?

COMMISSIONER CARR: Mr. Sands, yesterday we heard from a staff attorney; a lawyer in private practice; and one of your
colleagues, the federal defender from the Middle District of Florida, all of whom were listed as speaking on behalf of the Federal Public and Community Defenders. And I know that you're Chair of the Federal Defenders Sentencing Guidelines Committee. I'm trying to find out for whom you all speak. When I hear from someone from the Department of Justice, I know that that is the Department of Justice position, and I'm not going to hear something different from some U.S. attorney from Minnesota or California. And I'm just trying to find out how broad and formal is the representation of you and the others who speak on behalf of the federal public and community defenders.

MR. SANDS: The people that are here speak on behalf of themselves. We don't walk in lockstep as the Department, and we believe in giving the Commission a wide variety of views. Hopefully, everyone is consistent.

COMMISSIONER CARR: Okay. But
that's because you would anticipate sort of a similarity of views but not because the federal defenders across the country have been canvassed and have agreed that anyone [is] speaking with one voice?

MR. SANDS: That is correct. We intend to try to channel things through the Sentencing Committee. But, for example, if the Commission wants to hear from someone who actually does the submersible cases, it doesn't make sense for someone from Nebraska to do it. So that's why we bring those who have the expertise.

COMMISSIONER CARR: Thank you.

ACTING CHAIR HINOJOSA: I guess just a quick follow-up. If the Commission were to invite a certain public defender in a certain area, I know with the Justice Department it works differently, would we be able to do that, or do they have to get permission from someone in order to come -- let's say the Commission had identified a certain public defender who had expertise,
would they have to ask permission from some committee or someone else to be able to accept the invitation?

MR. SANDS: I'm available at any time, Chair. No. If the Commission reaches out to a specific defender or an assistant defender, then that's the Commission's prerogative.

ACTING CHAIR HINOJOSA: Commissioner Howell?

COMMISSIONER HOWELL: Yes. I just wanted to explore what seems to be a little bit of a difference of opinion on this panel, which I think is fairly interesting and one of the issues that the Commission is grappling with. So I want to direct this to Mr. Prout. To be honest, I sort of share Mr. Bussert's and Dr. Scalora's sort of concern about ICE, you know, focusing on internet communications for some kind of particular enhancement when it comes to threats. And I just wanted to explore with you for a second the differentiation that you make between internet
postings either on blogs, websites, and so on, and threats that are made over radio and TV.

From my perspective, I mean it seems to me that the concern about not knowing who the audience is who is listening is a far more concern with radio threats or television threats than internet threats where you can actually see who's actually accessing a blog or accessing a web site through logs of originating IP addresses of people who are visiting, people who post on blogs leave digital footprints all over the place. So in some ways it's a lot easier to track the audience of internet postings in a variety of fora than it is to figure out who's been listening to a radio threat or a TV broadcast threat.

So I was actually interested in your view in your statement that the Marshals take internet threats so much more seriously than TV or radio threats. Could you explain that a little bit more?

MR. PROUT: Yes, ma'am. Thank you
for the opportunity. My first comment on that, as you spoke about television and radio, was that there is regulation in television and radio. If somebody incites violence or threatens an individual over the television, the FCC monitors this stuff, and there are rules about it. That is not where the dramatic challenge comes from. The dramatic challenge comes from the incite and call to violence that these individuals are making.

Our challenge over taking these threats so seriously is our need to reverse actually a cultural movement in that if one individual manages through blog postings to draw out hundreds of others to make phone calls, to come out in person to visit judges and prosecutors to have their say, and those visits, those attempts, those endeavors are recognizing a growing intensity of effort. The intensity of effort may be by first a collective, then we must draw down to figure out who the individuals are that are actually exercising this.
The challenge over the threats of the internet, at first, over investigation, I recognize the conflict you see, we can identify who makes postings when we're aware of which would be millions of websites to go to. But we can[not] identify who might be called to violence based on those postings. So that is where the extraordinary resources wind up focusing on: the unknown.

The individuals that make those postings are well aware that they may be making a veiled or an individually to themselves empty threat. They may never follow up on their own statements on the internet, on television, or radio. It is the call to violence that incites others that is the dramatic concern of the Marshals Service and the Department of Justice.

VICE CHAIR CASTILLO: My personal problem is what do we do with those individuals that post personal residential addresses without calling for an incitement of violence but, nevertheless, posted in a way
that it can get to somebody who has violence in mind? And it seems to me that somebody who makes a post like that has to accept a responsibility for making that posting with the chance that violence might come with that because of the nature of the internet. And I'm just wondering if you have any reaction to that, especially Mr. Prout or Dr. Scalora. Do you think that that is just off, or do you think that it's acceptable for an organization like ours to just attribute that type of responsibility for those type of postings? Because, ultimately, it's the posting of personal information that I think leads to violence. That's what we found out in Chicago, in particular.

MR. PROUT: I'll defer to Dr. Scalora. I definitely have comments on this, but since I got to talk last I'll let him talk first.

DR. SCALORA: And to be clear, while I am always a little weary of focusing on one modality, I do support the Marshals'
concern about the use of the web or any electronic communications as a means of campaign of incitement. And I think those are issues that are extremely difficult for agencies to manage. And so to the degree that the Commission were to look at this and find strategies to address this, I think any type of effort to incite I think would need to be taken seriously. I think focusing on certain types of technology I think is a challenging way to go. That is not necessarily disagreeing with the Marshals' concern about how some of these things could go to audiences we may not be able to track.

VICE CHAIR CASTILLO: But what about no effort to incite but just a posting of a personal residence? To me, it's almost the equivalent of putting a gallon of gasoline in front of somebody that could be a arsonist, you know. It has a twisted potential to it.

DR. SCALORA: I agree, your Honor. I think for us we tend to look at the context. If, for example, hypothetically speaking, a
government official was in a news story and
the subsequent blogs had a rather intense
spade of negative comments, frankly at most
public sites those would be filtered out. So
let's say we're going to a more private
website/blog that's encouraging these things.
I think an individual who just says here's
judge so-and-so's address, minus those issues
I think it would be a much harder thing to
suggest that they're somehow engaging in a
campaign of harassment, intimidation, or
whatever. I think that individual who happens
to say, "I don't know what should happen to
judge so-and-so, but, by the way, here's his
address," and this comes after several dozen
rather insidious comments, I think that
context is substantially different.

And I'm not a prosecutor and would
not even claim to know how they do their job.
I don't know if that's prosecutable or
provable. I think from a contextual point of
view, that is substantially different than
someone who puts it in more in isolation
because I think, to use your example, someone putting gasoline just out in the corner, harder to argue. Someone doing it and you're at an arsonist convention, I think it's an easier call in that respect.

MR. PROUT: If I may follow-up, personally, my opinion of what you describe would be that person is dancing around the law. They are putting that can of gasoline out there allowing others to light it. And, unfortunately, that is a tactic of these individuals, of these groups, just put enough information out there, it's just free speech. If the Washington Post can put it out there, why can't I? That exists. These individuals are playing that.

Oftentimes, there is the inciters and the little rabble-rousers behind them, and that occurs. And those often differentiate where we come in with inappropriate communications versus threats. The release of restricted personal information with the intent to do harm is actually covered by the
code, and we find it to be rather, you know, somewhere in there is, usually looped, some form of threat.

Releasing that information with just dropping it out there we have to deal with as an inappropriate communication, expend the resource to determine, first protect to figure out if it's going to result in some hearing the call to violence by another individual just by reading that address plus other postings that may lead a person to a collective thought. We have to expend the extraordinary resources to determine if that call to violence is going to come, and that means risk management, mitigation, and protection of all the potential individuals involved: family members, the judiciary, the prosecutors, or our own agents, depending on the case.

MR. SANDS: But is it really worth doing that complexity or having an SOC for that? It could be an accidental. There was an instance in Phoenix in which a public
official owned property that was the subject of some dispute. His name was placed [inaudible] there a huge uproar because it was Sheriff Joe Arpaio. Do we really want to deal with that? Mistakes happen. And, again, this is an area that a judge has the flexibility to address.

VICE CHAIR CASTILLO: What I hear both Mr. Sands and Mr. Bussert saying is it doesn't need a uniform guideline change, but a judge can use their upward departure discretion for the isolated egregious cases. Is that basically it?

MR. BUSSERT: I think it is, your Honor. And part of the trouble I have, I guess, in the Marshals' presentation is one of the examples cited is someone goes on the radio and says the judge lives here or whomever lives here and then goes and posts on the blog. Well, how do we distinguish if someone acted where they heard it and what caused them to act when we get into situations where people broadcast, which they
increasingly do, terrestrial radio via the internet or they post transcripts, like Rush Limbaugh does, on his radio broadcast and then it's freely available?

What about situations like Michael Phelps? You say things don't find a way on the internet. They do. Michael Phelps was at a party in South Carolina, and the next thing you know is his photograph is shared with the entire world. Things happen outside of the world of the internet that perhaps there's no intention they're going to find a way on there but increasingly they do through Youtube and all these other forms. And we're viewing this in a very murky area in terms of trying to punish what could be very much innocuous behavior, and I think the doctor makes the very interesting, I think, telling point to focus on the behavior and not the modality, and the people that are going to engage in this behavior and the way that the Commission would be concerned about are going to employ a number of modalities. They're not going to
simply be based on the internet or based in the mail or whatever it may be. They're going to use what's at their disposal.

ACTING CHAIR HINOJOSA: Doctor?

DR. SCALORA: Sir, if I may, I understand the deep pain that recent events, especially directed toward members of a judiciary and their family, have caused in terms of recent acts of violence. That being said, I have looked at public officials across different branches of government, particularly on the legislative side, but at different levels of government, and one of the things I've also noticed is that sometimes the protectees are their own worst enemy. And I don't say this to be disrespectful or flippant, but if I could find out a judge's address by pulling out the white pages, some of this is moot at some level. We're expending a great deal of energy to protect people who may not always be doing things to protect themselves.

By no means am I suggesting they
are responsible for the things that are happening to them, but some of this information is not that difficult to find. And I think if one was to truly be effective in this regard, I do think punishment needs to fit the crime, and I realize you're working at this end of it. And I know federal judiciaries have heightened concern and sensitivity to these issues, but I think some of these issues can also be addressed substantially through preventive efforts by not making some of this information as readily available as it can be. Frankly, they would have a harder time in Lincoln, Nebraska finding my address than they would of some of our judiciary, and I say that with deep respect for our judiciary.

And so sometimes our efforts may have to be directed elsewhere. Thank you.

ACTING CHAIR HINOJOSA: Go ahead.

And then Commissioner Wroblewski afterwards.

VICE CHAIR SESSIONS: Can I just respond to that? I agree that we need to be
much more preventive, but what really is the
cconcern is when somebody puts the address on
the internet or in the open public in the
context in which it is presented and the
implicit message is that there should be a
threat or should be taken as a threat. And,
you know, that's irrespective of whether you
could actually find the address in a telephone
book. I mean, that's actually the harm.
After all, we're talking about sentencing and
persons convicted of a crime, and it really is
that implicit intent to cause harm or create
reckless environments in which harm could
happen. I think that's a little different
than, you know, something that you could
prevent.

DR. SCALORA: No disagreement,
your Honor. My point is that we could create
a very elaborate and sophisticated strategy
that we could end up defeating ourselves with
not considering other things. And no argument
with your concern. I spent my life doing this
kind of research, consulting with agencies who
try to prevent these things, so we're singing
from the same pew, sir.

    MR. BUSsert: Two points on that.

Again, I think, one, we have to have an
appreciation for technology and where we're
moving, not where we're coming from but where
we're moving. And if you look now in
retrospect at the child pornography guidelines
in particular, there's a two-level enhancement
for use of computers. In reality, in this day
and age, pretty much all of those cases happen
via computers. It's not an aggravating factor
in and of itself, yet the two-level
enhancement is still there. I think judges
are increasingly disagreeing with that.

    And I think the second part is one
of deterrence, which is to suggest that some
esoteric kind of two-level bump in a
guidelines manual that a lot of attorneys
can't even understand, yet alone some person
who's kind of a rabble-rouser or has this in
their mind is going to be deterred in any
meaningful way. I think we're not really
thinking in the larger picture, and I think Mr. Sands spoke about this kind of looking at the broader view in terms of where we're going. A lot of this is talking about preventative measures relative to punishments, but what we're really talking about is an enhanced punishment as some level of general deterrence. The populations that I've heard about, at least that we're referring to today, don't seem like they're very rational people.

VICE CHAIR SESSIONS: Actually, Mr. Sands said that I said that, that we should be thinking about --

MR. BUSSERT: Yes, and it was a very good point.

VICE CHAIR SESSIONS: Didn't you say that?

MR. SANDS: Absolutely, Judge. We should follow it.

COMMISSIONER WROBLEWSKI: Can I follow up on that, if I could? And this is a question for Jon. You mentioned at the beginning of your testimony about the
cumulative impact of individual enhancements and the need for a systemic review of the guidelines and severity levels.

One of your colleagues yesterday also talked about the need to focus on certainty of punishment as much or more than the severity of punishment. We share many of those concerns. And back in August, when we sent the letter to the Commission on our priorities, we asked the Commission to undertake a systemic review of the guidelines. And for that and for many other reasons, the Commission has begun a process of reviewing the guidelines as a whole. As you know, there was a regional hearing in Atlanta.

What was disappointing, though, is the colleagues of yours who testified at that regional hearing suggested that no systemic changes actually were necessary, that they were suggesting that the Commission focus crime by crime, individual crime one at a time. And that was very disappointing, and it seems inconsistent with what you're saying.
here. Could you address that? And am I
getting the wrong message?

MR. SANDS: Yes.

ACTING CHAIR HINOJOSA: It's
actually a regional hearing question, but I'll
let you go ahead and respond.

MR. SANDS: Well, part of the
regional hearings was the Commission asked for
line attorneys, for people who are in that
region addressing certain issues. We try to
address that. And this goes back to who the
Commission wants. The Commission has worked
with us, and we hope the Commission would
defer to us and work through us about who we
would pick, but we pick these people or we ask
them to testify to address issues that were
rising in that region and what they testify
to.

There are others that deal with it
on a national level that can deal with a
systemic change. Yesterday, Donna Elm talked
about how minor role is never given in Tampa.

It is an 11(c)1c stipulation in the District
of Arizona for drug cases. So you see these
different things, so that's why you need a
sentencing research council and you need a
national view. And we'd be happy to work with
you on a systemic change. Trust us.

ACTING CHAIR HINOJOSA: One of the
comments that was made, and I think it was
you, Mr. Sands, about how we shouldn't rely on
any individual case. But it seems to me that
almost every, at least you all tend to give us
an individual case scenario with regards to
whenever you give a statement to the
Commission, as did the defenders yesterday and
the prosecutors do the same.

I guess my question is you
indicated that we shouldn't really listen to
that, and so my question is why do people
insist on doing that and what should we do
with that?

MR. SANDS: I didn't do it.

ACTING CHAIR HINOJOSA: Well, you
just did, I think, in response to one of the
questions --
MR. SANDS: Sure. And that was in a response --

ACTING CHAIR HINOJOSA: But it was a specific case, and so --

MR. SANDS: It gives color. It gives a way of looking at a specific situation, but it doesn't replace 20 years of data of trends, 20 years of research by the doctor at the end of the table, or the experience of a number of investigations that the Marshal undertakes. So you have to look at the whole thing. Policy should not be by anecdote. Policy should not be by bias and --

ACTING CHAIR HINOJOSA: No, I'm agreeing with that. I'm just saying that, traditionally, from the defense bar we usually hear that, as we do from others. And I'm not disagreeing with what you're saying. I'm just saying that we are subjected to that on a pretty regular basis.

MR. SANDS: Well, they're good stories, too, Judge.

ACTING CHAIR HINOJOSA: Yes, they
are. But the point is then you don't really
know the background of each case.

COMMISSIONER HOWELL: Can I just
follow up a little bit with Mr. Sands? And
this is a continuation of the conversation
that I and some other Commissioners were
having with one of the federal public
defenders who testified yesterday specifically
focused on the Commission only taking steps to
respond to congressional directives if
empirical data, whatever that meant, and that
was an interesting exploration of discussion
yesterday, as well. And I just wanted to go
back to your opening comments, too, because
it's clearly a theme of the federal public
defenders right now where you said that the
Commission should only take action guided by
our seminal statutes, you know, 3553 and 994.
And you didn't leave much room for current
congressional actions, for example
congressional directives that we're grappling
with right now that explicitly direct the
Commission to increase penalties for certain
crimes.

We don't view those kinds of explicit congressional directives which are different from other kinds of directives which basically ask the Commission to review and consider, if appropriate, in each guideline changes. When Congress tells us specifically and explicitly to increase penalties, we also feel that that's a law we have to follow under the guidance that we've [been] given. We've been given in 3553 and 994 to follow the law. And it just seems -- could you just explain what the federal public defender view is about how the Commission should deal with explicit directives from Congress to increase penalties in certain areas?

MR. SANDS: You have to look at the interrelationship between the Commission as an expert body charged with knowing about sentencing and Congress that is acting. So if Congress just gives a general directive, it is one thing. If it's a specific directive saying increase it by this level, then the
Commission has to give that great deference. So the Commission, as an independent agency, can say, "Congress, you are wrong." It would have to be an important and supported issue, but the Commission should just not be a skimmer for Congress, and the Commission has never been that. And so Congress says increase this penalty, then the Commission should look at it, see if it's warranted, see what increase might be there, and, if it feels it is not, ask Congress to study it more or ask Congress to reconsider. It's not bad to have a dialogue.

VICE CHAIR CASTILLO: Before we leave today, I do want to get back to the issue of Native American Indians because I'm very sensitive and I think this Commission is. We've had an advisory group in the past. It almost sounds like you're suggesting that we should have a permanent advisory group. Other than the three issues that are up this time, we now have a victims advisory group. Are you suggesting that we should have a permanent
advisory group for Native American Indian issues? That question I'm addressing to Mr. Sands and Mr. Stegman.

MR. SANDS: I'll let Mr. Stegman go first.

MR. STEGMAN: Well, I can say I don't think it would be a terrible idea. I think that these issues are going to continue to come up on a regular basis. I mentioned the NIJ study that's going to be coming out. It's going to shed a lot of light. We're looking at every arm of the criminal justice process.

In Indian country, we're interviewing federal, state, tribal, everyday citizens on reservations. And issues come up all the time about sentencing on a regular basis, about what needs to happen. And, you know, a lot of these issues are especially difficult unless you have people really speaking and advising from that situation. You know, these are very tightknit communities, very family-oriented, and a lot
of times you end up affecting the victims just
as badly as you do the defendants with certain
sentencing decisions because, you know, we
mentioned domestic violence cases, child abuse
cases. They're all very much affected by
federal law.

And like I say, typically the
states and much more localized sort of
entities tend to deal with a lot of these
cases for non-Indians, but for Indians they're
very much interacting with the federal
agencies and the judiciary. So I definitely
think there would be a lot of value in it
because almost any of these criminal decisions
that come up under federal law are going to
always implicate tribes in a very different
way.

MR. SANDS: And as the Commission
might know, there's a major Indian crime bill
that will be introduced soon by Senator Dorgan
that will have a tremendous impact on federal
jurisdiction.

ACTING CHAIR HINOJOSA: Does
anybody else have any questions? If not, thank you all very much. We appreciate your advice and counsel and appreciate your taking your time to be here today.

(Whereupon, the above-entitled matter was concluded at 9:46 a.m.)