Day Two—Plenary Session VII

Understanding New Technology Offenses

Moderator: **The Honorable Michael E. O'Neill**, *Assistant Professor of Law, George Mason University School of Law and Commissioner, U.S. Sentencing Commission*

Scott Charney, Esq., *PricewaterhouseCoopers*

Mark Rasch, Esq., *Vice President for Cyberlaw, Global Integrity*

Howard Schmidt, *Corporate Security Officer, Microsoft Corporation*

Martha Stansell-Gamm, Esq., *Chief, Computer Crime and Intellectual Property Section U.S. Department of Justice*

PLENARY SESSION VII:
UNDERSTANDING NEW TECHNOLOGY OFFENSES

PROFESSOR O'NEILL: We are turning now, at least in part, from some of the more specific discussions involving the guidelines and some of the background with respect to the scope of cybercrime and the difficulties inherent in cybercrime, both in terms of its detection and prosecution and how the sentencing guidelines will apply to those types of crimes, to the understanding of new technology offenses.

I think we have been able to put together quite an interesting panel to talk about some of these different issues.

I would like to first introduce Mr. Scott Charney, who heads the Digital Risk Management and Forensics Practice for PricewaterhouseCoopers. Mr. Charney formally served as chief of the Computer Crime and Intellectual Property Section in the Justice Department's Criminal Division from 1991 to 1999. In this role, he was responsible for implementing the Department's Computer Crime and Intellectual Property initiatives.

Next, we have Mark Rasch, who is vice president of Global Integrity. He, also, like Mr. Charney, headed up the Department of Justice's Computer Crime Section, even before there was a Computer Crime Section.

Howard Schmidt is both the corporate security officer for Microsoft Corporation and the international president of the Information Systems Security Association. In that capacity, he directs activity for those responsible for the security of Microsoft information, personnel, and facilities worldwide.

Prior to that, he was the director of the Air Force Office of Special Investigations, Computer Forensic Lab, in the Computer Crime and Information Warfare Center. In that office, he specialized in conducting investigations into intrusions in government and military systems by unauthorized persons in counterintelligence and criminal investigations.

Of course, last but not least, we have Marty Stansell-Gamm who is the current chief of the Justice Department's Computer Crime and Intellectual Property Section. I think, in looking around here at this panel, she probably sees her future. She joined the original Computer Crime unit back in 1991, and among her many duties, she served as the working group chair and editor for the Justice Department's *Federal Guidelines for Searching and Seizing Computers*; she has represented the United States at the Council of Europe on Technology Crime Issues since 1992.

She coordinated the investigation that led to the 1995 arrest of that notorious hacker, Kevin Mitnick, and directed the Department's support of investigation into the "I Love You" virus which, as we all know, caused a great deal of havoc on the net.

It is interesting to me that we live today in an increasingly interconnected world that presents unusual opportunities. I remember back, when I was about 14 years old, I was with a group of my friends; a bunch of other 14-year-old boys. In that group of friends, there was one 15-year-old girl. Not unlike what 14-year-old boys are want to do, we all very much wanted to impress that 15-year-old girl. To do so—we had a little abandoned vacuum cleaner factory near where we lived—we decided to show our

prowess of throwing rocks through the windows to see which of us could nail the most glass, cause the most damage to this abandoned vacuum cleaner factory.

Well, back then, that was still a naughty thing to do, and I think my dad punished me. I think it was sort of a bad situation, all in all, but the amount of damage that I could do was considerably limited.

Let's fast-forward that to today where, if you are a disgruntled 15-year-old, you can throw a rock not only through the windows of an abandoned vacuum cleaner factory but through Microsoft Windows; you can cause enormous unintended loss and enormous damage to a system that is vital to this nation's national security, that is vital to our economic backbone and to the worldwide web itself, all without necessarily having any more intent to do damage than the damage that I did as a 14-year-old budding juvenile delinquent, I guess.

The issues that we have to deal with, particularly the issues of loss—be it intended loss or unintended loss—are absolutely central to understanding and getting our minds around the concept of cybercrime and the potential that it has for enormous damage.

One of the things that I would like to focus on, as we enter our discussion today, is also the problem of informational attacks. How many of you here read either *The Washington Post*, *The New York Times*, or *The Wall Street Journal*? Just a show of hands.

A pretty good chunk of people here read one of those three newspapers. What would you do if two days before the presidential election you read on the Internet on your favorite newspaper's website that George Bush had had an inappropriate liaison with a teenage campaign worker? Or two days before the presidential election that Al Gore acknowledged accepting bribes from Chinese officials for favors?

Now, I think that we depend upon *The New York Times* or *The Wall Street Journal* or other information sources to ferret out the truth for us and to provide us with information as accurate as possible. But, with the Internet and with worldwide manipulation of information and attacks upon information, we can dramatically affect events, stock prices, and other questions that are fundamental not only to e-commerce but to privacy and to other questions.

A little bit earlier today, we talked about the problem of obscenity. You know, it is possible to go through surfing the web, taking pictures of young children—at least taking their heads and cropping those heads off and placing them on adult bodies—and then distributing not just a single picture to 100 or 200 people but literally to millions of people throughout the world, in a way that, simply, ten years ago was absolutely impossible.

Well, if I happen to be a budding anarchist, think that all software ought to be free, and put a copy of Windows up for free on the web for people to download—even though I have no intended gain and don't plan on any gain—the potential harm to Microsoft is far, far greater than if I broke into my local CompUSA and made off with half a dozen copies of Microsoft Windows.

So, with these questions establishing some of the concerns that we have with respect to cybercrime and the worldwide web itself, I would like to turn, first, to Mr. Charney for his presentation.

MR. CHARNEY: Thank you. This panel is on new technology offenses and sentencing. But, the first thing I actually want to do is put new technology offenses into some sort of conceptual framework. When you think about how to sentence people and figure out what is appropriate for the conduct, you have to first think about how the technology was abused and whether existing sentencing schemes actually make much sense.

From a high-level perspective, there are two major roles that we think about when we think about computers being involved in crime: one, is the computer as both tool and target—what we call the hacker cases, where people are attacking CIA, confidentiality, integrity, and availability.

Confidentiality is simply that data should be seen by only authorized users. Integrity is that it should be altered by only authorized users. And availability is that data should be available on demand to authorized users.

Then the second major role is computers as tools to facilitate traditional offenses such as the distribution of child pornography or fraud. To some extent, when you think about computers as tools to facilitate traditional offenses, you can look at existing sentencing and say, "Well, if it is a fraud case and the fraud guideline looks at the amount of loss, we can use loss as an effective measure of the scope of the crime."

But, in the CIA cases, it is actually far more difficult than that. Because in these kinds of cases, the kinds of harms that can occur are so varied and so seldom look alike. The philosophy of the sentencing guidelines is to treat similar people similarly and it is really, really hard to do that.

Let me give you some examples. On the confidentiality side, we are talking about people having access to data that they are not supposed to have. Well, many years ago, someone hacked into a hospital in Pittsburgh to steal a country western singer's medical record for sale to a tabloid. So you have a major privacy violation affecting someone's medical condition.

The value of that information? Well, one way to look at it is to say, "Well, what was the tabloid willing to pay for it?" On the other hand, if you are the victim of that kind of offense, the market value may not represent its true harm to you, in terms of reputation and otherwise.

When you think about integrity offenses, you see that people sometimes alter data in visible ways and, sometimes, in ways not meant to be seen. By way of example again, many years ago, the Justice Department website was hacked and they took down Janet Reno's picture and they put up Adolph Hitler's picture, and we knew right away. It is meant to be seen. It is kind of like graffiti, and you fix it.

On the other hand, you may have situations where data is altered in subtle ways not meant to be seen. For example, we had a case where a hacker tried to get into a courthouse to commute his own sentence from prison to probation.

Now, it is a great plan because, in fact, we rely on data in computers all the time, with the underlying assumption that it has not been unduly tampered with. Just think about how many times a day you look at some information on a computer screen and make some kind of decision based on the reliability of that information and never question whether that information may have been tampered with.

The difficulty is, though, for that kind of integrity offense, how do you value it for purposes of sentencing? If someone tries to commute his sentence, what value does that have? How do you figure out what the harm is? And, what if someone else changes some other data for another purpose? For example, we had someone who accessed a bulletin board service. The service gave buy and sell recommendations for mutual funds. This was a disgruntled former employee, and he switched the buy and sell recommendations.

Now, the fact remains that even if you could show some sort of harm, how do you take that and the reputational value of the company and the subscriber base that says, "You know, we rely on your recommendations. We didn't realize they weren't to be trusted." So there are some very difficult issues.

And then, in the availability area, it becomes in some respects the hardest of all; in large part, because so many of the denial of service attacks and availability issues have impacts sometimes far broader than the actor intended. And because of the nature of the Internet and the way things propagate, even little things become huge things very, very quickly.

You know, as far back as the "Morris worm," where Robert Morris, Jr. prepared a little code and then it ran amok and, in about 24 hours, shut down 6,000 computers around the world; how much of this do you hold this person accountable for in terms of sentencing?

If you look at the way viruses propagate, you know, somebody writes a piece of code, and the next thing you know you have estimates of incredible damage, $80 million or more. If you just look at that kind of result and apply it to the sentencing table, what you are going to get is everybody getting life sentences all the time, and that may not be appropriate.

Now, one of the difficulties with availability, too—and it is important to understand this issue that Mike Vatis talked about about—is critical infrastructure protection. Simply put, we are now heavily dependent on information technology systems for public safety, national security and economic prosperity.

And the concern is that the disruption of these systems will have a dramatic impact on our way of life. And it is not just, of course, that these key networks will go down, but there are concerns about cascading effect; how does a shutdown of one network affect other networks? If telecom goes down, how do you do banking and finance when the banking and finance community is reliant on telecom for electronic funds transfer?

Again, this is not a hypothetical problem because there was a hacker in Massachusetts, a juvenile, who shut down a telecom—thus denying telecommunications service to some people in the town of Worcester, Massachusetts. But, unfortunately, this switch also served a local unmanned airport. When planes came in, they would radio the tower, and the tower would send a signal across the telecommunications network to turn on the landing lights on the runway.

So, as the next plane came in and radioed the tower, because the telecom switch was disabled, the landing lights didn't go on, the airport had to be closed, and planes had to be diverted.

But, when you look at that and say, "Okay, how do you sentence this person?" Leaving aside the fact that he was a juvenile, even if this were an adult, how do you equate for fairness in sentencing the

shutdown of an airport with the shutdown of the phone service, Robert Morris in 1988, or the "I Love You" virus, more recently?

So there are going to be some very, very difficult issues because what people want in sentencing is a sense of equity; that is, people who do bad things get certain sentences, and people who do worse things get bigger sentences. And the difficulty is, what constitutes a worse thing and is this worse thing that happened really what the person intended? And to what extent should people be held responsible for the ultimate result, even if maybe they didn't foresee as clearly as they should have—especially if they are young—that there could be this cascading effect and this huge problem?

It is important to remember, too, that what we have done in the Internet and in the computer generation, as a whole, is we have given extremely powerful technology to everyone on the planet. I mean, essentially, we have given every citizen a weapon of war. We normally don't do things like that. And, to the extent that we have done it, we now have a very large population base, globally located, that can cause incredible damage, for which there is really no comparable past experience.

For example, many years ago, you may remember, a Korean passenger liner was shot down. Everyone thought the Russians had done it. The Russians denied it. Finally, the Russians admitted it. Everyone knew it was military-state action or rogue-military action. Why? Because individuals don't have access to fighter jets, so it had to be government-related.

That is not true anymore. If someone with a computer can cause a plane to crash by disrupting an airport, you can't make the assumption that it is state action or military action. It could be a juvenile. It could be a terrorist. Or it could still be a nation state. So, as these cases unfold, you have to figure out how to sentence them, and it becomes very, very difficult.

Let me end by basically highlighting one or two issues that I think we need to think of as a group. The first one is the public perception of a lot of these crimes. I think there was a question to Richard Power earlier, about the $10 billion of estimated loss from some of the denial of service attacks. There are a lot of people I talked to who basically say, "So what? The economy survived. The companies survived. What is the problem?"

And we do have a lot of expansion and elasticity in this economy to survive those incidents. To the extent the public doesn't see these things as very serious, the question is: how does the judiciary react? I mean, part of leadership is sometimes being ahead of the public perception.

But, on the other hand, you run the risk that, if you are very harsh in your sentencing, people think it is disproportionate to the crime that is committed.

The second problem is: how are we going to quantify losses? How are we going to quantify them in economic cases, such as in the "I Love You" virus or distributed denial of service attack, when most companies actually don't do reliable damage assessments? Most of the statistics you read are really guesses, and the information is not particularly reliable.

How are we going to quantify non-economic losses: the theft of a medical record, the invasion of privacy, a denial of service attack where you don't have much damage on one end because of lack of damage assessments and the defendant didn't profit? The switch of the buy-sell recommendations—are we

going to calculate in the reputational damage? Is that going to be the only damage if none of the investors actually took any of the loss? Or do you say, "No one took any loss; it is a non-event?"

And, if you say that and you suggest to people that if the ultimate result isn't really negative—you are not going to be punished—then you are sending a different and dangerous message.

The other issue to think about is scope. The denial of service attacks via "Lovebug"— these were global events. To what extent are we going to calculate in global harms as part of this process? Are we going to expect every country to prosecute the defendant and each get their piece of this person for the damage he did in that country, or are we going to start thinking about how to aggregate the losses in one country and maybe sentence him there for the good of the entire planet?

And what are we going to do with the non-profit cases, the younger hackers who don't have motives like economic gain that can be easily quantified, to move forward and figure out what a reasonable sentence will be?

So it seems to me those are some of the biggest issues. And, I guess, the one last one is: how do we figure out what particular damage to attribute to a particular defendant for purposes of sentencing? If you remember, after some of these virus attacks, very quickly out come mutated versions, slightly changed. Is the defendant who created the original virus responsible for all of that?

Many years ago, we did cases where people were posting telephone access codes to bulletin board services so they could be downloaded, so that people could make free phone calls. When we arrested some of these defendants, we went to the phone company and said, "How much loss have you had from these codes?" And we had a list of codes from the bulletin board. And they could say, "We had four million dollars of losses because that is how many phone calls were made with these codes in the 30 days before we shut it down."

You go, "Okay, but how many of these losses are attributable to this defendant?" Because he posted on a bulletin board, other people copied the board *en masse*. It distributes like a web, just out. And, all of the sudden, you say, "Well, were these calls made on the 25th day a direct responsibility of this individual?" The answer is: you don't know and you can't prove it. So we are also going to figure out, in these big widespread events that have lots of tentacles, how much is attributable to the actor that we have gone after.

PROFESSOR O'NEILL: Thank you, Mr. Charney. If we could turn, then to Mr. Rasch?

MR. RASCH: I promised Michael that I would be controversial, so I start by being controversial with a disclaimer that my opinions may not be my own.

Now, I was struck listening to the last two speakers, particularly David, about what the structure of the guidelines are for the various computer crime offenses, and Scott, about the subtleties involved in computer crime, with this huge dichotomy between the certainty that is required by the sentencing guidelines, that sort of rigid slot machine approach to deciding people's fate and the incredible subtlety and difficulty of trying to come up with these sentences.

Then you go back to the issue of the purpose of the sentencing guidelines which are, essentially, to provide some degree of consistency, some degree of certainty, some degree of deterrence, and you realize that those two concepts don't merge together well at all.

You can have two identical facts, two similar facts, resulting in widely divergent sentences, based upon the intent of the prosecution, the diligence of the prosecution, the ability to gather the evidence of loss, what the victim decided to do, and how the they decided to react to the offense and the like.

What we end up with is—when presented with a particular fact pattern about a particular computer crime case—a visceral gut reaction; this is a bad person who did a bad thing; this is not a bad person who did a bad thing; or this is a bad person who did something that wasn't so terrible.

We can't necessarily decide why that is, and in almost every regard, I disagree with the calculations that the sentencing guidelines come up with. Take a look, for example, at child pornography; I think we can all agree that child pornography is bad, but we can't necessarily all agree why child pornography is bad.

The original reason child pornography, for example, was bad was that in that order to create child pornography, you had to commit the crime of child abuse. We start with the assumption that some child pornography is obscenity. And then there is a degree of child pornography that is constitutionally protected free speech because pornography is free speech, but is illegal because a child was involved.

So the original purpose of the child pornography laws, at least as applied to pornographic images of children and not obscene images of children, was to deter the child abuse inherent in making the images. We have now blurred that distinction with the Virtual Child Pornography Statute where no child may have been involved in the making of the images.

The second question is, why is somebody who has eight images worse than somebody who has 18 images? These are all value judgments we have to make. Is it worse if somebody downloads them all at one time or downloads them over a period of time? So, what we have done is we have sacrificed being right at the altar of being consistent and are at the altar of the easy approach.

So we simply say, if you have more than a certain number of images, then you get an enhancement. Rather than looking at the subtlety and saying, "Wait a second, is this a bad child pornographer or is this just a guy who happened to be cruising and downloaded a couple of images?"

Is there any empirical evidence that people who download child pornography are more likely to become pedophiles or be pedophiles and act on those tendencies? If so, sentence them for that. I mean, that is really what we are interested in—protecting children, not protecting adults from viewing images of children. If that is true, then let's add some subtleties to the guidelines and allow us to sentence them for what they have really done and why they really harm society.

If you look in the area of the loss guidelines, again as Scott was talking about, if you look at the denial of service attacks, you can have an instance where you have Michael throwing rocks. Michael throws that rock and, unbeknownst to him, there is some volatile substance sitting on the floor of this factory. Suddenly, the factory goes into flames. Michael runs like hell and gets caught.

Suddenly, not just the factory burns down but a couple of houses nearby burn down. Does Michael spend ten years in jail for something unknown to him? And the answer is, "Yes." We recognize that it is much more serious as a consequence of what he has done. But, is it the same as if Michael wanted to burn down those houses and lit a match to do so?

So we have circumstances where the sentencing guidelines will dramatically overstate the seriousness of the offense. I think the Robert Morris case was such an offense. I think the "I Love You" virus may be such an offense, depending on the values of losses.

And you have other circumstances where the sentencing guidelines may dramatically understate the seriousness of the offenses. Again, what we have done is we lack subtlety. We lack the ability to make those kinds of sentences in the way the sentencing guidelines are currently structured, unless we start departing wholeheartedly.

And the example that I tried to pin David down on is the question of: if the government comes by and says, "I downloaded a file"—it cost $1.7 million to download the file, by the way; there is case called *Riggs & Nydorf* which presents this in an unfortunately dramatic fashion—"isn't the difference why did I do it and what did I do with the information that I downloaded?" If I am just a kid, and I download the formula for Coca-Cola, a very valuable trade secret, and read it and say, "Oh, my God, that is what they have in it. I am never drinking Coke again."

The loss is, of course, the cost of resecuring the trade secret and preventing its further disclosure, as well as maybe the lost sales from this kid. However, the loss is not going to be the $20 million or $50 million that might happen if RC or Pepsi did the same thing.

So, by just simply looking at the one factor—what is the value of the information?—we lack the subtlety to decide what is the seriousness of the offense.

The same thing is true in crimes like the Emulex fraud and cases like that, where we simply look at the issue of loss. Because what we almost always do is we take the largest number we can. Prosecutors typically they lack the ability under the sentencing guidelines—unless they are going to play fast and loose with the facts—to say something like we had to do in the Morris case.

In the Robert Morris case, he did a worm that caused anywhere up to $90 million worth of loss. But he didn't intend to cause any loss or much loss; he just wanted to see if this could be done. What do you do in a situation like that? Do you sentence this person as if they had stolen $96 million? Did the kid in Canada, Mafiaboy, who did the denial of service attack, really steal one billion dollars? Would you sentence him as if he had stolen one billion dollars?

On the other hand, in the case involving the singer, we also don't take into account other losses; the main ones are loss of confidence in both a company and in the technology that may result, as well as loss of privacy.

So what we have done is we have come up with some fairly narrow categories that we are going to use and say, "We are not going look at everything else." What we really need to do is say, "Make the sentencing guidelines exactly what they should be, which is guidelines." These are some factors that you

should look at, but you can look at other factors and really make a determination how bad this person is? How bad this crime is, in context?

For example, if somebody puts one copy of Microsoft Windows on a computer for download and six people download it and then 9,000 people download it from the other sites, are you going to hold the individual responsible?

There is an assumption made in the guidelines that everybody who downloads pirated software or a song from Napster would have purchased it at its full purchase price. Can you diminish the value of the loss by saying, "You know what? The guy downloaded the pirated copy of Windows, and then he liked it so much he went out and bought it."

So, what you recognize is there may be a distinction between "I post a copy on a bulletin board service so my friend can download it, and unbeknownst to me, 5,000 people also download it. Am I liable for that type of stuff?"

And we don't have answers to that, nor should we have answers to that, nor should the guidelines attempt to give us the answers. We do need to enable prosecutors, defense lawyers, and judges to make these decisions on a case-by-case basis. It is the only way that you are going to develop a consensus in a body of law. That is what I have to say.

MR. SCHMIDT: Thank you. I think I am going to take a bit of a direction here that is probably a little bit more tactical than my colleagues to my left have taken, thus far.

First, I want to frame for a moment where we have come on this thing, and we will talk about the Internet for a moment—the Internet, as Scott and Mark have mentioned, in the early days when we talk about the "Morris worm." I generally refer to that piece of the Internet as the basic plumbing. That is where the TCPIP, the transfer control protocol and all those things were developed. Fundamentally, they were there for research. They were there for some of the military use. But, effectively, it was just connecting terminals to mainframes and things of that nature.

Version 2 of the Internet was when we started actually moving, in the early '90s, to the dial-up systems where we actually had PCs in our homes and offices. We were using dial-up lines and talking to servers. The latter part of that generation, if you would, is when we laid on the web browsers and all this hypertext mark-up language with the rich content that we see out there and that sort of moved us to the era of looking to webpages for information.

Then the third piece of it is—and I think this is where we are at—the collaboration phase, where we depend on it. We have broadband technologies, DSL, cable modems, things of that nature. We are not only talking people to machine but, as Mike pointed out, machine to machine.

I get pages, sitting here, with updates of good things that are happening. I also get updates on weather and things like that, where my machine, based on the way I have it configured here on my hip, is conversing with other machines to provide me information without me having to out and look for it.

So, consequently, the whole nature of what I am doing now changes to where I am getting stuff pushed to me on a regular basis and becoming very dependent on it. To give you an example of how

dependent I have become on it—it used to be when I was in headquarters living in D.C.—that when I would travel somewhere, I would go to great efforts to print up maps. Now, of course, they are on the Internet. You can print up maps and take them with you.

So I would be driving down 495 with this package of paper sitting on the steering wheel trying to mark things off as to where I am going. This morning, when I left the hotel out at Tyson's Corner, I just punched in, in my little wireless device, the address here and told it go out and give me the step-by-step directions how to get there. I did not have a paper map. I depended on that service to be there to provide me the ability to get here on time for this symposium.

So, consequently, the level of dependency that we have on the Internet and the high tech devices upon which we have come to depend on is really crucial.

I want to take it one step further before I talk a little bit more about the loss versus the effect versus the gain, which I think is really salient to the discussions today, and talk about the next generation, the home things; and we are not so far from there now.

Envision for a moment that our vice president of Consumer Strategy has developed the *grocer.com* to find out, at seven o'clock, Thursday night, if you are available to have groceries delivered to you. That is the sort of technology that we are becoming more and more dependent on, and it is not that far down the road. It will be very commonplace.

The effect of the technology on sentencing is where I will specifically get into the loss versus the effect versus the gain. Let's talk about loss for a moment. If I ask any one of you in this room: if you could afford to lose one dollar to a fraud, a scam, just a downright theft—you leave a dollar on the table and someone takes it—is that going to have a major impact on your life? Probably not.

I raise that to ten dollars. At what level does the pain start to be felt? Fifty dollars? One hundred dollars? Of course, some of the students in here would drop back down to the ten-dollar level. But the bottom line is, there is a minimal effect on the threshold of pain that we have to deal with individually; it may not be very great in a lot of the instances that we are seeing in high tech crime.

Well, let's put that around a little bit and look at a million people losing a dollar to a criminal who is doing something online, who is somehow manipulating my services to where I am unable to make those investment decisions; I am unable to get those directions. There is not much of a monetary loss or a loss to me, personally, when I take 20 minutes longer to get there.

If you have an opportunity, the FTC had on the website the last time I looked, sort of the dirty dozen, the 12 top scams on the Internet out there. If you look at them, the vast majority of them are not designed to ruin your life. They are designed to get the $10, the $20, the $30, the $50 out of you, one million, 10 million, 20 million times over, because that is the audience you now have the ability to touch. It is not just one individual being affected.

You bring that back down to a lower level where we are talking about state and local jurisdictions, and I think back to the days when I was a police officer in Arizona many years ago. We changed our felony theft statute so the threshold went from $250 to $500; we did sort of an impromptu survey within the next year. You know what we found? Criminals were stealing stuff up to $499 in value. Because there

was sort of a threshold there they could anticipate. It is a misdemeanor if I am doing $499. It is a felony if I do $500. Didn't count taxes in there, I don't think, so we kind of left that $499 value.

And that is the same thing that we are seeing with some of the activity on the Internet. There is a threshold of pain that people will put up with. If we hit you up for $19.95, you go to your local police station, or you go into some local jurisdiction. They are not going to get too excited and go out there and track those people down, even though the gain that they may have realized might have been in the multi-, multi-millions of dollars.

Then, lastly, I want to talk about the effect of it, if I may. This other device that I have here, also, is with the technology. I have a wireless component to this where, as Mike alluded to, I can sit there and actually do transactions. Of course, being a security person and a law enforcement person most of my life, I don't have it to where if I lose this thing, nobody is going to be able to access my accounts because I don't save passwords and I don't do those basic security measures that we take care of. I don't do those things on a mobile device like this.

But, if you look at the analogy of the days when it was safe to run into the 7-11, grab your cup of coffee while the car is running to keep it heated during the wintertime in D.C., and come back out and expect to find your car there, those days are past.

It is just like the generation now where we have got to start training people. Don't leave your passwords and things like this on these devices. And here is why. Someone can grab one of these—and it has been done—and sell off every piece of thing that you have been working for your entire life, sell your entire portfolio. Some may be large; some may be small. The way the market has been recently, you may thank them or you may wish that they had let it sit until it makes the rebound as it oftentimes does.

But, consequently, they have no gain. You have a loss. But the effect is bigger than that. It goes back to solidifying the comments that Mark and Scott both made relative to the confidence level that you have. If I am not confident that my reputation, my personal finances, my medical records are going to be able to be secured and there is some deterrent out there to keep people from finding it fun to sell everything that you own, and then you come back and find out that you just took a $200,000 hit in your well-being, that is something that has got to be taken into consideration as far as sentencing goes, as well as the effect on the deterrence aspect.

I was interested in Mike Vatis's comment this morning about the "I Love You" virus because, when that virus first hit, I got the call a little bit after midnight, west coast time, and was told that it was taking place, running rampant through so many computer systems.

Within an hour and a half, we had notified the FBI, notified the Department of Defense, as well as the ISP in the Philippines, that this was going on and got them to shut down the site. For those of you who may not be familiar with the virus itself, in addition to the nuisance component of it and the destructive component locally, it also had a component where it would take passwords off your system and mail it to this site in the Philippines.

We were able to get that site shut down, after we notified the FBI, within an hour after this thing is running rampant. Therefore, we were able to save—using that same technology that creates these problems—a whole lot of people from having problems because it was turned off in a moment's notice.

So that is the boon and bane of this whole thing. We have the negative component, but on the same token, we can use that same technology once something negative does happen, to be able to regroup from it in a relatively short fashion.

To be able to turn around and somehow refute that information on such a rapid basis does help and does need to be taken into consideration on some of these things. Thank you, Mike.

PROFESSOR O'NEILL: Thank you very much. Now I would like to turn, last but not least, to the Department of Justice to see what their take is on this.

MS. STANSELL-GAMM: One of the things that you seem to be hearing from all of us is that, as these new technology offenses begin to become more common and as we see patterns in them, we are all saying that many of these are big and many of them are bad, but it is hard to quantify exactly how big and how bad they are. I think there is agreement among us that it is going to be tough for the sentencing guidelines, in a quantifiable way, to measure this.

In addition, I would like to point out a couple of other attributes of these offenses that make our task even tougher. Scott alluded to one of them, and I would like to pick up where he left off. He mentioned that technology offenses are different in many ways because the instrument of the activity, the computer, is a common, everyday thing. You know, it is not registered. It is not regulated, and nobody is proposing that it should be. But it is something that is not unique to a certain set or class of individuals. The source can come from anywhere.

This makes it very, very difficult at the beginning of a series of events to know what is going on. So, really, what I would like to say to you is: when we ask how bad this offense was, really there are almost two sets of answers. The first is at the beginning, and the second is at the end. And, oftentimes, those look vastly different.

I will give you another example. This is common in hacker attacks on the Department of Defense, but several years ago, some of you may recall, a hacker attack occurred during a time of Gulf War deployment. The hacker attack was a little unusual because, first of all, the activity was sudden, concerted, and widespread; and it focused on a certain kind of server, a domain name server in the military that is essentially responsible for routing Internet traffic. Those domain name servers are the ones that translate *www.cybercrime.gov* into the numeric address.

So, if the domain name servers were to go down all at once, the traffic would be greatly disrupted, or maybe the whole network would go down. The Department of Defense was deeply alarmed by this, deeply alarmed. It is hard for me to fully convey to you the scope of the threat they perceived.

In the course of several days, what we were able to ascertain was that much of the activity appeared to be coming from computers overseas and specifically from the Middle East. The war fighters in the military were probably jumping the gun by wanting to engage in information warfare because, when we were finally able to trace it all the way back, it turned out to be attributable to two teenagers in Northern California and a young man in Israel who was in his early ‹20s.

Now, a lot of people take a look at it and say, "Well, those silly guys in the Department of Defense, don't they just blow problems up. What were they thinking? They were wanting to engage in information warfare with teenagers in Northern California."

Well, that, of course, was not what they thought was happening. And I guess what I want to make clear is that, at the beginning of one of these events, it is very difficult to tell in looking at the audit logs whether this is a national security emergency or, as somebody else mentioned earlier—I think it was Richard Power—a commercial competitor—if it is a business—or teenagers looking for trophies or having fun.

Those audit trails look alike. For the same reason, we think that pulling fire alarms as a prank is not very funny. But this is a much, much bigger fire alarm, and in fact, if the Department of Defense domain name servers had been under attack from hackers in the Middle East, all of us would have been testifying before Congress if we had said, "You know what, it is probably kids." You know that is right.

So, there is a huge amount of noise on the network—if you want to call juvenile pranksterism noise—that looks very, very serious, causes actual damage, and is indistinguishable at the beginning of the investigation from other kinds of more serious activity.

I will give you one other example. A company called the FBI in an absolute froth some years ago because the crown jewels of their source code program had been downloaded from the network. They had just turned down an offer, a multi-, multi-million dollar offer, to sell this source code to a foreign government. They were not sure, of course, who had stolen the source code, but they feared the worst, and they came to the FBI because they needed the answer to that. They needed to know whether it was a competitor, the foreign government, or kids.

Again, it turned out to be kids. What is the damage from that? Somebody said, "You know, maybe it is the damage of the kids' not drinking Pepsi or Coke." But I think you ought to add in the medical care for the system administrator who had cardiac arrest when he saw that that material had been downloaded.

So that is a real problem because a lot of folks want to look at the case at the end of the day, when the investigation is over, the conduct has been attributed, and say, "Ah, it is just kids, it is all right." But that attitude has significant infrastructure protection consequences.

Now, on the other hand, I would never suggest that the appropriate response is to boil the kids in oil, you know. That is too much, too. But, one of the problems that we have is a significant, I think, public misperception about whose fault these things are. Whose fault is it when some of these events occur?

One of the things I think we all hear a lot is that it is the fault of the tech industry. These tools, the software, the hardware, are manufactured quickly. They are manufactured irresponsibly. They have got holes in them. They are all buggy. And it is really the fault of the tech industry, and we ought to be mad at them.

Some people say it is the fault of the moronic victims who buy the tools from the tech industry and don't know how to implement them. They will set up a computer server with the default password still operational, and somebody can log on, "guest-guest" or "root-root," and they will get right in. So it is the victim's fault.

Now, this is fodder for many, many interesting conversations about where responsibility lies. My own view is that some of those are going to be settled or will shake out civilly. Another way of saying it is we all expect our banks to use reasonable security. We don't expect our banks to have perfect security. We all sort of intuitively know that, if our branch banks had perfect security, they would all look like Fort Knox and we wouldn't be able to get in and out of them ourselves.

Security is expensive and it is inconvenient. Security is the opposite of access. So the more secure a place is, either physically or electronically, the harder it is for authorized users to get in and out of it and the more it costs to secure the network.

So I would love to see a public understanding that security and access are in this sort of tension and that we, as a society, are going to hold responsible people who breech security, even when it is not perfect. For example, let's say a robber robs a bank. Maybe the security of the bank is not what it should be. Maybe it was unreasonable and there are going to be some consequences of that, but none of us are confused when it comes time to sit on a jury or to sentence a criminal about whose fault it really is. You know, we are prepared to hold the criminal responsible.

Another way of saying it is, "It is not okay to do stuff just because you can." So there is no permission to hack systems, abuse systems, steal information just because it is possible to do it. Of course, it is possible to do it. These computer systems are never going to be perfectly secure because we couldn't stand it and because they are, after all, designed and used by people, and there are ways of entry when people are in charge.

The other thing I would like to comment on—and then I know you would like to have a general conversation—is the problem of the foreseeability of the conduct. All the previous speakers have given you some very interesting examples of cases in which people—again, they have a tendency to be kids or young adults—engage in conduct, the consequences of which surprise them or appear to surprise them.

Scott told you the story of the teenager in Massachusetts who disabled the switch. In fact, what happened was he got root on the switch and a message popped up, "Would you like to re-initialize this switch? Y/N." And he said, "Y." That was it. So it wasn't as if he said, "You know what, I am going to take down telephone service." It wasn't at all clear that he even knew what the consequence was. So I think we have some very serious questions about whether the consequences of electronic activity, in fact, surprise people or whether, as a matter of reasonableness, they should surprise people.

It may be that, as the society becomes more and more sophisticated about the technology, as we all become more enthusiastic users, we will all begin to understand that there are probably going to be consequences for hitting the "Y."

There are certainly other cases—maybe not in the federal guidelines, but certainly in state law—where we do hold people responsible criminally for what we consider to be the foreseeable consequence of choices. One of the simplest is drunk driving or reckless driving.

I used to be a defense counsel when I was active duty in the Air Force, and I can't tell you how many people I worked with who came to me and said, "You know, I was drinking and I didn't intend to drive drunk, and I certainly didn't mean"—I had this happen, once—"to hit the kid. That wasn't what I meant to do. I love children. I didn't mean to hit the child."

And the answer is, our law, as a public policy says, "If you make the decision to drink and you make the decision to drive, you are going to be criminally liable at some level—not for first degree murder—but you are going to be criminally liable at some level for what society says are the foreseeable consequences of this, even though you, personally, would never intend this."

And the reason we do this is because we want people to make different decisions when they have the opportunity to do it. So, over time, what I would expect is that society would begin to say, "Don't hit that button; don't you press that "Y," because, even if you, personally, did not intend to take down the telephone service of Worchester, Massachusetts, and the airport with it, that is, in fact, a foreseeable consequence."

So that is going to be an interesting social evolution. These do present fascinating problems for us in making punishments fit crimes.

QUESTIONER: I don't know if Mark is going to like this comment or dislike it, but it seems to me that a lot of the conversation suggests that the guideline system with a well-functioning departure mechanism is exactly the way to start developing consensus about how to deal with all of these uncertainties.

The rapid changes, the range of offenses and offenders, mean that it is going to be very difficult for the Commission now, and even going forward, to develop formal, highly detailed rules that will capture all of the nuances, all the subtleties, as I think you put it, in all these cases.

But the best way to have an active dialogue between judges, the Commission, the Congress, and the entire society about these issues is to have the Commission sort of tentatively get started and then encourage judges to depart, both upward and downward, in all of these cases, based on their case-specific perspective on how this is going.

At one point, you sort of disparaged departures or said it won't work unless we have departures going. But I would like to hear your comments, in general, and Commissioner O'Neill's views, also, about whether that may be the best way in which to start dealing with all these subtleties.

MR. RASCH: I would tend to agree with that. I think that what the guidelines ought to be is some basic framework of the types of factors you need to consider.

One of the things I get from the discussions I hear is, "Get rid of loss and gain; talk about consequences." Consequences are a lot different than simply economic loss and gain.

Economic loss an gain is a function of the civil system to sort of recoup losses. It is not necessarily appropriate in the criminal system. Loss or gain are some consequences to these actions, but privacy and integrity and confidence are other consequences.

So we should talk not of loss and gain in the computer crime context, but rather of consequences, and we should set out specific factors. I don't think that you can say an invasion of privacy is a two-point enhancement or a five-point enhancement. You just say it is an enhancement. You may depart and enhance based upon loss of privacy. You may depart downward based upon the fact that the actual consequences are much greater than the defendant's intended consequences, all right.

The example Howard gave about stealing one dollar from each person—imagine if you caused a loss of one dollar to a million people, but had no profit. Under the way the guidelines are currently structured, you get sentenced for a million dollar crime. That is because we have these rigid guidelines to try to promote certainty.

The other problem with the concept of trying to promote certainty in this area is, if I were to give you a fact pattern that I could make up off the top of my head right now and tell you that these are the facts that you are required to find, and ask you what is the sentence, I can almost guarantee you that every single one of you will give me a different sentence.

For example, if you have a script kiddie that somebody just downloads stuff off the web and launches it, is that more than minimal planning? Is that a use of a special skill? Or has the Internet become so ubiquitous and these tools so ubiquitous that that skill is no longer all that special anymore?

And you make value judgments, and the idea of the guidelines has sort of set a framework for those value judgments. Get people thinking about what those value judgments are, but allow liberal departures. Now, one of the problems is we have this adversarial system where we fight tooth and nail over departures. A defense lawyer will fight tooth and nail over any upward departure, saying that it is unjustified, and it will almost inevitably result in an appeal, and the same thing the other way.

Rather than getting a general consensus, I think this is the right thing to do—which is, of course, what the sentences were—how they tended to be before the guidelines.

MR. CHARNEY: I would like to add one point just to clarify because, actually, some of this has already been done. The Sentencing Commission revised the sentences for computer crimes on November 1st of 1996. It was originally a Justice Department proposal, and then there was a working group at the Commission. We went back and forth on a lot of these issues.

We, ultimately, concluded that certain things, like invasion of privacy, could not be a two-point adjustment. In fact, there is a departure provision for invasion of privacy that allows the parties and ultimately the court to decide how bad the invasion is and what the departure should be like.

Even damage caused by the cutting of a telephone line, although it may cost $500 to fix the telephone line, may have denied service to lots of people for a long time and $500 might not be an accurate reflection of the consequences.

So, just in the interest of full disclosure, the Commission has looked at this and incorporated some of the things that we are talking about here.

PROFESSOR O'NEILL: That is right. I think one of the other difficulties that we get into, a lot of this, it seems to me, is an educational informational problem. If you recall, the guidelines were originally structured on the basis of what the received wisdom of the bench and bar already was; what do the judges generally think a bank robber, under particular circumstances, ought to get sentenced for.

In states, when we talk about harm, manslaughter, an unintentional homicide, how much is a death worth? Well, over time, we have developed principles that guide us, that inform us, as to what a loss of life is worth or what a loss of limb is worth.

Probably, the difficulty that we have in this area is that we don't have sufficient experience or received wisdom for people to know what the consequences of their actions may be. Because 20 years ago the way drunk drivers were treated is not the same way that we treat drunk drivers today, there has been a long educational, informational process to bring people up to speed, to understand that these are not your mother's drunk driving laws that we have today.

The difficulty we have in this area is that the pace with which change occurs is so incredibly swift that the informational component, in being able to disseminate this information among people, always has an enormous lag time because things are always changing quite rapidly.

So we are caught in kind of a difficult situation. This is probably heresy to say, I suppose, since I am on the Sentencing Commission, but it is my belief that a lot of these areas want to give judges a lot of discretion over time and see how it shakes out.

To me, the common law is, ultimately, the greatest social science research experiment. The common law is the received wisdom of a lot of smart people, over time, dealing with real problems and coming up with solutions. And it seems to me that this might be an area that is absolutely ripe for allowing a certain amount of discretion to see how all these things shake out, and to allow private industry to unite with the government to get out there to teach people that, "Hey, it is wrong to download software. It is wrong to punch that ‹Yes' button on your keyboard. It is wrong to turn somebody's computer into a slave of your master so that you can have a DDOS attack; that those things are wrong." And that kind of educational component is something that is simply going to take time.

MR. SCHMIDT: I think I would like to add on to the education component and, having been involved in a number of criminal as well as civil cases where I am trying to educate the judiciary on some of the technical aspects, I agree very, very much that there has got to be a process in place to make sure that the benefit of that education then helps rule some of the decisions that are made.

I think in a lot of the high technology cases that are going on, people oftentimes walk away going, "I am not sure they really understood what this particular technology meant in the decision that was made."

Particularly, in some of the criminal cases I have been involved with, you walk away with that sense that there is going to be a decision made without full realization of the information that was conveyed during the trial. So I think, full heartedly, that there is an educational process that needs to go on with that.

I was contacted a number of years ago by National Judicial College, down at Reno, to put on some classes, just sort of teach—and this was back in the early '90s—some of the technology issues. And I think that is another thing that is going to help because, if you understand the technology, the departures upward or downward from whatever the guidelines might be become more relevant and more defensible, particularly when it goes into the appellate issues.

MS. STANSELL-GAMM: I just would like to agree with the comments that have been made and say that there is a general lack of understanding about what the code of conduct, if you will, should be on networks.

A couple of years ago, I got a call from a NASA agent who said, "You are not going to believe this: we got an e-mail from a graduate student at a technical university who said, ‹You morons, I hacked you.'"

And, apparently, the system administrator didn't respond quickly enough and so the student came back and said, "You idiots, you didn't fix the hole. I hacked you, again."

It is the sort of thing that makes you want to say, "Where are their mothers? Don't they understand that this is not the right thing to do?" But, if you read the popular press, you will hear this attitude expressed, regularly, that somehow hackers think they are doing us a favor by pointing out the holes in our systems.

My response is that that makes about as much sense as sending thank you notes to burglars for pointing out the infirmities in our alarms. If we didn't have burglars, we wouldn't need alarms.

So there is some real ethical confusion on the network that is crying out for adult presence.

MR. RASCH: The adults aren't any better.

MS. STANSELL-GAMM: And, of course, some of the activity is, as we heard this morning, no kidding, for-profit, with "I want to hurt you for gain" criminals and, obviously, the sort of thing I am talking about doesn't address that.

But, you know, when we hand the keys to a car to our kids, we teach them not only how to protect themselves, but we teach them that they have a huge responsibility to protect other people. And grown-ups are just not doing that with the technology because most of us don't recognize that they could hurt other people. It is not part of our experience, and so it is not one of the things on our checklist.

PROFESSOR O'NEILL: And this just goes back to one of the difficulties with intent and how we determine intent in the world of cybercrime.

MR. RASCH: And motive—I mean, would you sentence this kid who kept telling NASA, "Hey, fix the hole," the same as the kid who doesn't ever tell NASA that he found the hole and exploits it? So one of the things that is missing from the guidelines is the concept of motive.

PROFESSOR O'NEILL: And, certainly, the Cult of The Dead Cow thinks it is doing the world a great favor.

QUESTIONER: I just wanted to respond a little bit to what was just said because it seems to point out the dichotomy, which is that, on the one hand, the use of the computer is very frustrating to law enforcement and makes their job quite hard, and the question of what should be prosecuted, what should be prohibited, is in flux.

That doesn't get to the question of sentencing. Sentencing is about making moral choices and right and wrong and punishment. And I haven't heard anything that suggests that using a computer to steal money or using a computer to commit vandalism is worse than vandalism or theft.

If you are going to use a sentencing structure, what I don't understand is why you add two points to use a computer for child pornography rather than doing child pornography, or it is two points worse to infringe a copyright through the computer than to infringe a copyright?

I would suggest that, in dealing with all of this, the Commission should be very careful in going for those easy enhancements because it is a computer, because it is frustrating, because it is worrisome that the consequences might be incalculable when, in fact, it is not that different than the same type of wrong conducted without the computer.

MR. RASCH: Let me address that because I am glad you brought that up. That is one of the things that bothered me about the guidelines.

The answer is that it can be worse because you use the computer, but it isn't always going to be worse. Which would you think is worse, some guy sitting in his living room downloading kiddie porn or some guy arranging a conference at George Mason University for people to exchange kiddie porn in person? I mean, the answer is we have to make a value judgment about which one is worse.

QUESTIONER: I have had the experience of representing people accused of kiddie porn in the pre-Internet and post-Internet world, and the fascinating thing for me to find out was what you had said, Mark, which is that the images are no longer the same.

I mean, when they were doing sting operations, with real magazines with real pictures of real people, you at least knew where the pictures came from and that there was an element of child abuse. Now, you have bulletin boards with thousands and thousands of horrible pictures; many, if not most of which, are not real anymore. And you have people now who can sit in their basements, download thousands of pictures, and be gratified in that way.

And the question of morality, the question of right and wrong and punishment is very complicated. And to just say because they can get more images now and because it is on the computer, it should be two points worse—I could sit here and make an argument—why shouldn't it be two points less; why the computer has made that world in some ways a more benign one, if that is possible.

MR. RASCH: I think, in the kiddie porn area, that is something with a lot of subtlety, and we need to do some studies, sociologically, and get the database so we can make that value judgment, rather than simply taking the easy road and saying two-point enhancement.

In many, many cases, the use of the computer to facilitate it does make the crime worse because of the anonymity afforded by the computer, the speed of committing the crime. You could not commit an "Emulex" kind of fraud without the use of the computer and computer technologies and things like that.

So I think that a court should be entitled to take that into account as a factor, but I don't think the mere fact that you used a computer in furtherance of the crime or even the mere fact that you used encryption to conceal the furtherance of the crime, as opposed to using any other thing—let's face it, criminals don't want to get caught—and the fact that you didn't want to get caught should increase your penalty because you made it hard to catch you?

If that is your value judgment, then you say that in every criminal case. If you are taking any substantial step to prevent yourself from getting caught, two-point enhancement. Why use encryption as the scapegoat?

PROFESSOR O'NEILL: Well, we do the same thing with firearms. If you use a firearm, it somehow makes it more dangerous, for example, or if you have more than minimal planning.

MR. RASCH: Well, I am scared if you point a gun at me. I am not scared if you point "crypto" at me.

PROFESSOR O'NEILL: No, but I suppose the argument is that if you make it that much more difficult, maybe it is deserving of some sort of enhancement.

At least using a sentencing enhancement rather than raising the penalty from the get-go gets around the dual use problem; we want to encourage the use of encryption technology because it makes it easier to engage in commercial transactions on the net, but at the same time we don't want encourage the use of encryption technology for drug dealers who are trying to hide their illegal activities.

MR. RASCH: Well, if you want to have an obstruction of justice enhancement—and that is to say that, if during the course of committing the crime, you obstruct justice; or, if you just want to say concealment as an enhancement—that is fine and leave the technology out of it and the methodology out of it.

But what you are really trying to do is actually send an affirmative message, "Don't use ‹crypto.'" Now, when you say, "Don't use guns," there is a very good reason to say don't use guns in the commission of a crime.

PROFESSOR O'NEILL: Well, there may be a need, just in the informational aspect of it. I think that is a good point. Maybe on the informational aspect, we need to use that. We need to make it more costly for the criminal who uses encryption technology because we want to decrease the costs. . . .

MR. RASCH: I'll give you an example though. I file a fraudulent tax return and I encrypt it when I send it to the IRS in order to digitally sign it. I have now used encryption in the furtherance of criminal activity.

It is going to happen more and more often that encryption will further criminal activity, even communications about criminal activity and the like. And we are going to get to a point where it will be so ubiquitous that it shouldn't be. . . .

PROFESSOR O'NEILL: Maybe the case is more like a car or is it more like a gun, that it becomes so ubiquitous that we don't give an enhancement for use of a car, for example, in a bank robbery, but we do for use of a gun.

I think those are the precise questions that we need more data on, that we need to do a sort of shakeout of the system. Because, certainly, if the Sentencing Commission doesn't at least think about it, I can guarantee you that Congress is thinking about it.

MS. STANSELL-GAMM: If I may just say, I want to make it clear that I don't necessarily disagree with you. I think, oftentimes, focusing on the technology can lead us in the wrong direction. I think what we are all experiencing and expressing is that the use of the computer oftentimes changes either

the degree of damage or the nature of the damage or the degree of difficulty in investigating and prosecuting the case.

And I think that there are a number of right ways to look at this, and we are probably better off by looking at those underlying values—degree of difficulty, degree of damage, scope of the activity—rather than just saying automatically up or down because you have used a telephone or a computer. So I don't disagree with you.

MR. RASCH: The only thing I would add at this point is that I would also get rid of the six-month mandatory minimums. If the calculations of the sentencing guidelines come down to zero, then so be it. You have made the value judgments in the guidelines. If you don't like the way it comes out in the end, then increase the guidelines to reflect enough factors or allow some more liberal departures.

But what we tend to do is not put caps on these things. We don't say, "If the guidelines come out higher than we like, you can't give higher than that." Congress does that.

And the other point is that—and Michael will appreciate this having worked on the Hill—once we have come up with this wonderfully elegant system and we have decided all the factors and we have got it all down perfect, Congress says, "We need to get tough on ‹X' and such," and suddenly Firestone executives are going to jail and things like that.

So we also need to worry about pressures, external pressures that have a tendency to corrupt sort of the intellectual process of trying to decide what to do, the right thing.

MS. STANSELL-GAMM: As some of you probably know, those mandatory minimums are a statutory requirement, and our section in the Department has been trying to change that, without success, so far.

PROFESSOR O'NEILL: I would like to thank each of these panel members for what was a most interesting and enlightening discussion.