Day Two—Hacking/Viruses/
Interrupted Computer Service/Intrusions/Privacy

Group Breakout Session One

Moderator: **Elizabeth Banker, Esq.**, *Corporate Counsel, Yahoo!, Inc.*

James Dempsey, Esq., *Senior Staff Counsel, Center for Democracy and Technology*

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

John Tritak, Esq., *Director, Critical Infrastructure Assurance Office*

GROUP ONE: HACKING/VIRUSES/ INTERRUPTED COMPUTER SERVICE/INTRUSIONS/PRIVACY

MS. BANKER: Good afternoon to everyone. We are going to get started with a panel discussion this afternoon on the sentencing issues related to a specific group of new technology crimes—specifically, viruses, denial of service attacks, and privacy-type related crimes.

My name is Elizabeth Banker. I am corporate counsel for Yahoo! I handle a variety of issues at Yahoo!, many of them related to privacy and security and working with law enforcement when it is doing investigations.

Also on the panel this afternoon, sitting directly next to me, is James Dempsey from the Center for Democracy and Technology. He has been there for over three years. At CDT, Jim works on electronic surveillance and Fourth Amendment issues. He has also written on those issues and spent some time working on a variety of issues on the Hill, as assistant counsel to the House Judiciary Subcommittee on Civil and Constitutional Rights.

Sitting next to Jim is Marty Stansell-Gamm, from the Department of Justice. Many of you are probably are already familiar with her, as she spoke earlier today. Marty is the chief of the Justice Department's Computer Crime and Intellectual Property Section. I am not going to bore you with any further introductions because I don't think she needs one.

Then, at the end of the table, is John Tritak. John is the director of the Critical Infrastructure Assurance Office. He has been there for over a year, and before that, he practiced law at Vernor Liipfert and spent some time at the State Department.

With that, what I would like to do this afternoon is start off with each of our panelists just making some general remarks about the topic at hand—which is related to figuring out issues related to harm and loss associated with these new technology crimes—and describing the crimes that we are talking about and some of the unique aspects of them.

MR. DEMPSEY: Thank you, Elizabeth. Good afternoon, everybody. I am not at all an expert in the guidelines so forgive me if I say anything that is inconsistent with them or their direction, but I would hope to be able to talk a little bit about some broader issues, including some of the questions that were raised in the earlier panel, which I think also inform this discussion. As an overall theme, I think that the issue at hand and the issue for the Sentencing Commission and for members of the defense bar is to begin better defining what is different and what is not different about computer crime. I think that, so far, we haven't begun to solve that problem very well. Partly, that is because of the newness of the issue and the tendency to hype anything new and the exaggeration that goes with the media coverage of new issues.

I think that computer crime is less different in some ways than is imagined and is more different in other ways. Let me explain what I mean by that. This morning, there was discussion about the fact that theft of money by a computer is no different than theft of money by embezzlement and is no different than theft of money with a gun with the exception that the use of a gun can kill somebody.

But the theft is a theft. Sabotage of power supply can be carried out with a bomb or it can be carried out with a computer, but, in either case, it is sabotage—a disruption of electrical power supply. You

can also, by the way, disrupt the power supply with a computer unintentionally, in some cases, just as you can disrupt power supply unintentionally with a backhoe, which happens. Somebody digging a ditch several years ago brought down the air traffic control system for the northeast region. So intentionality, obviously, comes into play.

We have to think about what is different about these kinds of crimes. The mere fact that money is stolen with a computer or proprietary information is stolen or fraud is engaged in, similar to what you have in a telephone-based boiler room situation, I think it makes very little difference if those crimes if carried out by a computer.

I think there are two areas, though, that do merit more careful consideration, in terms of the different nature of computer crime.

The first is the question of whether computer crime is easier or harder to detect and prosecute. You hear the view, often stated, that computer crime is more difficult to investigate and prosecute. I actually don't see the evidence for that. I dispute that proposition. I think that the investigation and prosecution of computer crime is different, but I am not sure that it is harder. I think, in some respects, it is easier. Later on, I can cite some examples of what I mean by that.

Secondly, I think there is a difference between computer crime and other crime when you think about what should be the proper mix that we want to have as a society between the deterrent effect of the criminal justice system and the preventive measures that all of us expect to take and that society expects us to take in terms of avoiding or preventing crime. I think that certain features inherent in the nature of the computer and communication technology weigh in favor of solutions that lie in the hands of the private sector on the preventative side and should lead us to give less emphasis to the deterrent value of the investigative, prosecutorial approach.

Disproportionately, in this arena, the solutions to the threats, to the security problems, to the kinds of crime we are seeing, lie in the hands of the victims. This is not a blame-the-victim exercise, and it is not to say that there is not a role for law enforcement. But, when you measure what you can accomplish by prosecution versus what you can accomplish if the private sector and government were to build more secure systems, I conclude that the more productive solutions lie not in the criminal justice system, but in the development of more secure systems. And then the question becomes how do we promote the development of more secure systems.

Those are some of my overview comments, and I will leave it there, in terms of just a basic introduction, and yield to the others and then take some questions that Elizabeth has outlined.

MS. STANSELL-GAMM: Just a couple of comments. I disagree, completely, that investigating network crimes is easier than investigating real world crimes. Having worked with computer crimes now for nine years, I feel fairly sure of this.

I can give you examples in the real world of easy cases, too. When I was a young lawyer, one of my first tasks was to write an appeal for a guy who had robbed a bank, and he was identified when the law enforcement officers followed his footprints in the snow. They got to the house where he was hiding and that was about that. It had just snowed in northern Michigan and so it was pretty clear where he had gone.

Sometimes that happens with network crimes, too. Sometimes we get lucky. Sometimes there are trails. Sometimes there are fingerprints, electronic fingerprints. And the truth is that, whatever the crime you are investigating, you collect whatever evidence is available, and you put it together the best way you can.

There are several attributes of electronic crimes, though, that consistently make them harder. One is that the evidence is almost always far more dispersed. So, even if there is a single communication, oftentimes the evidence that will link the event to the actor is dispersed among several different communication service providers that form the chain. That is where there is just one actor.

Oftentimes, the activity is global and so we are dealing not only with different jurisdictions in the U.S., but with jurisdictions all over the world. You heard stories about that this morning.

The other thing that typically makes computer crimes really difficult is that the evidence is almost universally perishable. Now there is perishable evidence in the real world, too; hairs and fibers and blood may not be available if we don't collect them quickly and we don't collect them competently.

But there are other kinds of evidence that endure, and what we find in computer crimes or communication crimes is that the evidence is always inherently perishable. It is ones and zeros. And because there is such a volume of evidence on these communications networks, it is very difficult to find and obtain it fast enough.

So these are repeating problems that we have in attributing conduct to a particular person or set of people. Some of these are technical problems; some of them are problems of the legal infrastructure, and some of them are operational problems because we don't have competent or willing assistance in foreign countries, for example.

So what we are trying to do is deal with all of those at the same time. We are trying to look at technical tools. We are trying to look at the legal infrastructure, and we are trying to build our trained operational network. So that is, I think, an important consideration.

As I said earlier, I would not say that just because a computer is used that of necessity there ought to be any kind of enhancement in the guidelines. I think we ought to look to see whether the case was, in fact, more difficult or whether some of the other attributes were present. Sometimes they are, and sometimes they are not. But what I do want to say is those difficulties are a common pattern.

MR. TRITAK: One of the things I want to focus on to encourage discussion is the dealing with harms and how to stop or minimize the impact of those harms. In considering this focus, I want to say a little bit about my particular role in the federal government since it represents a slightly different perspective from perhaps what you have been hearing today. The Critical Infrastructure Assurance Office was created under a presidential directive a couple of years back and has the main responsibility for coordinating federal government policy and developing national awareness efforts across the country in the area of critical infrastructure protection.

The critical infrastructure, incidentally, includes the electric power grid, the telecommunications system, the IT networks, banking and financial services industry, transportation, water, oil, and gas.

Increasingly, these infrastructures—which are really the bedrock of our economy and our government—are increasingly reliant on information technologies, not only to support their operations, but actually to perform those operations. Many of these infrastructures were previously regulated and they were public utilities. They have now become deregulated, privatized, and in order to maintain profits where profit margins are very small, they are relying increasingly on information technology networks in order to remain competitive and deliver quick and efficient services.

I want to indicate that this reliance on information technology networks is not just about the Internet. It is a much broader set of information networks. They are increasingly becoming interconnected in a very complex web of a growing digital nervous system. So what you have is an increasing dependency, an interdependency throughout the economy and across the country.

As a result of that very reliance on IT, you are introducing new vulnerabilities that are a condition of being connected and going online. We know that there are people out there who are attempting to exploit those vulnerabilities for a variety of reasons, everything from kicks, for profit, to strategic and political gain.

As a result, the President created a Commission, and ultimately created my office along with a national coordinator in order to manage this problem. It starts from the premise that since most of this infrastructure is owned and operated by private industry, they ought to be taking the lead in managing the risk to that infrastructure, with government providing a supporting role as appropriate.

But let me just say that one of the serious problems about critical infrastructure and the way it is becoming connected is that, when disruptions are introduced, they can have serious cascading effects, not only within a particular industry sector, but across sectors. The complexity of the networks is such that people don't necessarily understand how it would play out or what the consequential downstream effects would be to the end-stream users.

So, one of the interesting things that struck me when I was reading some of the materials for these guidelines is that, to the extent that we become more dependent on these things, and to the extent that some individuals can do significant harm to the economy, taking advantage of interrelationships and creating cascading effects is how that is going to be reflected in sentencing guidelines if, in fact, it can be reflected at all.

Arguably, existing laws and sentencing guidelines associated with cyber violations are going to be adequate for many of the kinds of new problems that arise in the computer crimes area. But I would suggest to you that there is a newer area here that needs to be considered.

I am not sure that requires a new set of guidelines immediately, but I would suggest to you that the potential economic harms that can be done on a much broader level than is usually associated with any individual act is something that should certainly be considered as the Commission moves on in its deliberations on future guidelines. I think this is something that is not likely to go away; it is likely to become more serious.

One of the things that the administration is trying to do as much as possible, as I said, is look to the market. I think this is inherently a risk management problem where your principal goal is to prevent and deter attacks from occurring, and if they were to occur, prevent them from having adverse consequences.

So, one of the things that we have been trying to do is enlist the full forces of the market—not just the owners and operators of these infrastructures, but the risk managers, the insurance companies, Wall Street, and the like—to make clear that there are certain obligations that are expected of private industries who own and operate these things.

There are fiduciary duties. There are due care requirements. In addition to the concerns that corporate leaders generally have about not having their services disrupted—and quite frankly, an increasing concern that data about their customers may be obtained in an unauthorized manner—we believe it is a good step towards getting the market to bear as much of the burden as possible.

That said, I am fairly confident the market can't bear the whole burden even when the inclination to create a secure and trusting environment for electronic transactions is appreciated. Economic self interest will only take you so far. And, in certain cases, the need for national security in certain very select industry areas may require something more be done. I think that is where public/private partnering is essential to work out solution sets that address those issues.

But also, increasingly, as companies begin to appreciate their obligations, they want to make sure that those who are perpetrating these crimes are caught. I am increasingly hearing from companies that I didn't hear from last year, saying, "Okay, we are starting to get this. This is costly. What are you all doing to make sure that the people who are doing this are taken care of?"

And, of course, one of the biggest concerns is that you don't want international borders to create safe harbors. Increasingly, as I am sure Marty would attest, many of the serious problems that we have seen of late are really coming from overseas. So the activities that are being undertaken by the Justice Department, along with a number of international fora, the conventions and the like, are attempts to try to harmonize certain criminal laws and practices so that you don't, in effect, create safe harbors for wrongdoers. I think this is an important step.

But, you know, like everything, the implication of risk management is that there is an acknowledgment that there is no such thing as perfect security for many reasons; one, it may not be obtainable; secondly, if it were, it may not be affordable; and, thirdly, in certain cases, it may not be desirable, particularly if it is irreconcilable with core values that we all share.

So, as we go down this road, there are concerns, and I am very aware of many of those that Jim has expressed, not at this conference, but in the past. These are public policy choices, and they are serious choices that have to be addressed.

I would suggest to you, in terms of the roles of the Sentencing Commission, that we need to think very seriously and broadly about the ultimate implications of moving into an information age and how the sentencing guidelines are going to deal with these issues. It may turn out that, for a variety of reasons, it is very difficult to quantify harm or whatever, or to reflect those kinds of harms in sentencing guidelines.

But, to the extent that the sentencing guidelines do, in fact, reflect the seriousness of certain types of deliberate activity on the information superhighway, it is also an important indicator to the public, as well as industry, as to what standards of behavior they may need to reach to in order to be responsible players in their own right.

So, I think, with that, I will pass the floor back to you.

MS. BANKER: Thank you to each of you setting the table for the rest of the discussion. I think a lot of interesting points have been made already, and one of them that I would like to go back to is this idea of it being either harder or easier to detect certain types of the new technology crimes.

I think the ones that are on the table for us this afternoon are kind of interesting because some of them, the very nature of the crime itself is that it would be obvious; the denial of service, the virus, those are things that you are going to know. Web page vandalism is another thing where the whole intent is likely to create awareness that something has happened.

Other types of new technology crime—the privacy violations, some of the theft of intellectual property or people's private information—may not be immediately detectible.

Do you think that that is something that should be taken into account? Is that a dividing line between which types of offenses are more serious than others?

MR. DEMPSEY: I am not sure that difficulty of solving the crime should be a factor in sentencing.

MS. BANKER: What about the effort that someone would go to to hide the fact that he has committed the crime?

MR. DEMPSEY: It is an interesting question as to why the use of encryption is not more ubiquitous today, and there are a variety of reasons that one could hypothesize as to why it isn't. But there is this image of the future, perhaps short-term, perhaps more long-term, in which there is more widespread use of encryption, and I think it will be precisely in those situations where you have got a white collar crime situation where the person encrypts as a matter of course, and they are doing a lot of legitimate things with that encryption, and they are also using that encryption in the course of whatever bribery or price fixing or whatever sort of white collar crime they may be involved in.

Remember, the whole purpose of encryption is to prevent crime. We want people to encrypt more—certainly, if you are engaged in the transfer of proprietary information or sending financial information, I think it is crazy to send that kind of information unencrypted. There is actually a debate within the legal community that I haven't followed that closely, that says that lawyers conducting communications with their clients by Internet have an ethical obligation to encrypt in order to protect the confidentiality of those communications.

So, we are actually putting pressure on people to encrypt and to use encryption. If you think about Operation Ill Wind, which was the major procurement fraud investigation of ten years ago, the people there were all engaged in legitimate activity. They also happened to be engaged in illegal procurement fraud activity. Voice wiretapping was a major component of that investigation.

If that kind of investigation had occurred today, there is a high likelihood that a lot of those communications that those people were engaging in would be by e-mail. And there is a high likelihood that they would be using encryption provided by the U.S. government, which the U.S. government encouraged them to use in the course of performing their jobs as Defense Department officials and defense contractors.

I think a lot of those people drew very little distinction between their legal and illegal activity. It was part of their course of daily conduct, in terms of how they went about their daily business, in terms of granting and bidding for government contracts. I don't see how you could say that, in that case, use of encryption should somehow exacerbate the crime.

MR. TRITAK: I think that part of the answer to what you are suggesting is that you really can't divorce the methods from the intent behind what is trying to be accomplished.

I remember reading one of the papers in the booklets where they were talking about harm, and it was talking about what was intent and the rest. Let's say that the person's specific intent was to shut down an electric power plant. Let's say that the consequence of the act was to bring down the electric power grid. The perpetrator happened to pick a time where, essentially, redundancy was not available, and it had a rippling effect, which then resulted in a hospital not being able to answer 911 requests, which in turn resulted in people dying.

Now, part of assigning harm and blame is also foreseeability. Was that foreseeable? I can tell you right now that interdependencies and how they would play out in certain cases are not well understood at all. So, you may suggest that the initial attack was deliberate and the perpetrator knew what he was doing, but the consequential downstream effects might be unforeseeable and catastrophic.

MR. DEMPSEY: But how does that differ from the pre-computer situation where 15 years ago Kupperman and Livingstone and others were warning that there were five railroad bridges along the entire East Coast, any one of which, if it was knocked out, would disrupt all rail traffic? Or, if you attacked one particular power station with a bomb, you would have precisely the same massive cascading effect could occur? So the question is, "How is the computer different from the bomb?" Now, the computer allows you to do it remotely, which has a significance, although I don't know that that makes it a worse crime.

MR. TRITAK: Well, let me suggest the following. It may not be, but let me just play out your scenario a little bit. I think the difference has to do with the magnitude of the potential harm that one could cause on a much larger population than any individual could cause without the computer.

Now, you make a couple of arguments about single points of failure where you attach any one of those points, and all of a sudden everything goes down. And we are all aware of what happened in New York City many years ago when—I don't know if it was an ax or somebody hit it with a backhoe—all the electric power of New York City went out.

But the thing is, though, if the capability to do that is there, and the magnitude of the loss is quite great and the ease of doing it is greater than it was in the pre-computer world, the question is, "Does this pose a greater threat to the state or the economy, where people are saying that cyber-based crimes have to be specially treated precisely because the implications are much greater than they were before?"

Look, anyone can blow something up. But the fact is that there is a high cost of going out and blowing something up. The fact through computers it can be done remotely, the fact that it could be done from anywhere, creates a different kind of risk to society that is less obvious to the immediate public than the terrorist who decides he is going to go to the location of a target and run the risk of being caught or killed.

So I guess my point is that, at some stage, it doesn't matter whether it is different from the pre-years of IT even though we have to treat it differently.

MR. DEMPSEY: My question is, in recognizing those differences, is that where we want to put our societal priority in terms of avoiding those effects, particularly when the people in the best position to know what the potential cascading effects are, are the owners of those systems? Shouldn't we put equal if not greater emphasis on building more secure systems?

If someone commits a crime, go for him, Marty, get him, put him in jail.

MR. TRITAK: Let me just say one thing about that. If you are asking me, if I think owners and operators need to do more to manage the risk and to bear the full responsibility for depending increasingly on IT; I can't agree with you more, okay?

But I will tell you, chances are what will happen in an environment where security is improved is that only the more sophisticated types of hackers will succeed in causing disruption, not that hacking and cyber attacks will go away. So the same types of problems are still going to be there. It may turn out that you are going to have a special class of people; only a special class of people could actually pull off difficult cyber attacks in an environment where businesses are doing what they are supposed to do in the way of security based on market research and the possibility of liability and the like.

I don't think greater security is going to erase the potential problems of all cyber attacks. And the question is whether or not cyber attacks have to be treated differently, whether society will demand that they be treated differently because there is an enormous social cost associated with it.

MS. STANSELL-GAMM: I think in some ways, we are sort of agreeing with each other. I want to make one thing really clear, though. I think it is a false choice to say, "Should we be putting our priorities on securing systems and in encouraging owners and operators to make sure that their systems are not abused? Or should we be putting them on the criminal sanction? Should we be investigating activity? Should we be prosecuting criminals if we find them? Should we be thinking deeply about the sentencing guidelines for these offenses and how they work?"

If you ask me that question, my answer is, "Yes, of course, you do both." You have to do both. This is a networked problem. There isn't, as you would say, a single point of failure. There isn't a hub. There isn't one place where you can intersect it and fix it. This is a problem that requires us to do a lot of things all at the same time.

In law enforcement, in addition to actually investigating and prosecuting cases, we are focused on improving the legal infrastructure in our own country and internationally, and we are focused on trying to create a better operational network. Those are things that are within our responsibility and control to do. That is what we can contribute to make these networks more secure.

We can't do everything. We can't make sure that the private sector secures its networks better. That is not the role of law enforcement. You know, we are partners. At some point, I have to pass the baton to Howard Schmidt at Microsoft or Elizabeth Banker at Yahoo!, and I want them to pass it back to me.

The same is also true of the intelligence community, which has a huge role in this problem, and the war fighters for information warfare. All of us have our competencies. All of us have our ways of collecting and disseminating information. All of us have our missions on which we are focused. And what we have to do, all of us, is get our heads up and realize that we are not the only players on the field.

Otherwise, what happens is—and I have seen this over and over and over again in cases—we all look like five-year-olds playing soccer. We are all on top of the ball. Wherever the ball goes, there we all go, and we are kicking each other in the shins.

I think what we need to do—whatever our piece of this—is back off and play positions, use each others' strengths and competencies, and work together, and share information to the fullest possibility of the law, and think creatively about how to solve a networked problem in a networked fashion.

MS. BANKER: Marty, in terms of building the legal infrastructure, do you feel that the current sentencing guidelines take into account all of the harms that are caused by the new technology crimes as we are calling them today?

MS. STANSELL-GAMM: The sentencing guidelines were changed several years ago so it is possible to depart upward for privacy violations; it is possible to depart upward in damage cases for what I call public health and safety consequences; and the loss calculation does factor in system recovery costs, the costs to the victim in putting itself back together.

I am not aware of cases where we are seeing incorrect or disproportionate results. I think that flexibility has allowed judges to do what they think needs to be done. I think one of the huge difficulties under the guidelines is one we were talking about earlier, and that is, in a loss- driven case, how on earth do you value that? How are we going to begin to think about that in ways that capture the full harm but don't overstate it?

My colleague, Elliot Turrini, is an assistant U.S. attorney in New Jersey, and whenever you are interested in doing it, I know he would be prepared to talk about the loss calculation that they did in the "Melissa" virus case. Elliot was the prosecutor in that case.

MS. BANKER: I think that would be very interesting. I think we are getting him a microphone right now.

MS. STANSELL-GAMM: This is not a surprise to him, by the way. I told him I was going to do this.

MR. TURRINI: I found it a very, very interesting case. I am going to assume everybody knows what the "Melissa" virus was, and I am just going to go right to how in society we value the loss or the harm.

I am going to distinguish between loss and harm because the guidelines do. And I found this entire symposium very interesting from that perspective. And, if you accept that loss is a term of art defined in the guidelines in 2B1.1, and you don't overemphasize the importance of loss and equate loss with the sentence that a person is going to get—if you don't make those mistakes, you had better understand how the guidelines have been formulated or really are intended to be used.

Loss is one factor, and we have decided to pick monetary loss; so, in every case, you choose a monetary loss, and that is one factor that is considered by a sentencing judge in determining the ultimate sentence.

Okay, but now what does that create for law enforcement and for the judiciary? Well, in a case like the "Melissa" virus, you have worldwide impact, and no one has ever before tried to calculate the actual monetary loss to society of such a crime.

I didn't know how to do it, and there was no precedent on which to draw from. So, collectively, the Department of Justice had to put its head together and figure out what to do. And we looked to the private sector to see if there was anyone out there who had expertise, and there were a couple of companies who had been thinking about these issues.

But, when you step back and say, "Well, what is someone's economic incentive to be prepared to measure the damages that viruses cause?" Not a lot of economic incentive behind it, so you understand why there are not thousands of people working on these issues.

Well, why don't we just ask the people, big companies; ask them, "Well, what happened? How many computers were hit and what was your experience?" And what we found out was that nobody wanted to tell us. And to make it really simple, if you were the person in charge of security at a major corporation, do you want to admit that, while you were on watch, your company lost $4 million? No.

Do you have plausible deniability that you can sweep it under the rug and people above you are never really going to know? You do it.

Now, I am really speaking a little bit in hyperbole, but that is the general reaction we found which led us to think about using alternative means, such as a research survey where we use statistics. And we were preparing to do a full-blown survey, making it statistically valid, with the right frame, and getting the right experts to make sure that it was fair and accurate.

But then think about how much money that costs. It is a lot of money. Do you want your federal tax dollars spent in that way? Well, what it highlights, though, is that we as a society are only in our infancy in understanding the actual harm, damage, ramification, consequences, whichever term you want to use, from these virus cases. And, because we have sentencing guidelines that require us to make a loss determination, the issue comes up.

One of the many things I appreciate about the guidelines is that they allow for a reasonable estimate. When you look at that, what that means, and the way it will play out is whoever is the prosecutor and whoever is the judge really get to decide how much time and effort and resources are going to be spent in a specific case determining the loss, and the loss is a big factor.

So, I mean, there are a lot of things that we learn and I have. For anyone who is ever interested, I have lots of research on the actual specific parts of the guidelines and the language that is used, and I have some suggestions on how they will play out when these issues are litigated forcefully.

Now they are not going to be litigated in the "Melissa" virus case because, as of public record, the defendant, David Smith, pled guilty. And he stipulated that his crime caused over $80 million in damage, thus saving a lot of time and effort by the federal judiciary and the Department of Justice.

MS. BANKER: The $80 million figure, where did that come from? I have seen it in the press. I think, with the "I love you" virus, I have seen numbers that were all over the place. One was even as high as $10 billion which included, you know, lost work time.

What goes into those figures? And for a prosecutor, if you are seeing numbers that are in the press and can't get actual numbers from victim companies, where would you go for the data?

MR. TURRINI: I have two answers. First, I would defer to one of the commissioners as to who wrote the loss table. Because if you look at the loss table, the highest number is $80 million. So, if you want to get rid of a case quickly and avoid some time and effort, the parties can say, "Yes, the damage was over $80 million," and you don't have to calculate whether it was $600 million, you know, $81 million.

Because the way the guidelines are structured is that, if the prosecutor decides that the loss is so big—it is $5 billion—then a prosecutor can seek an upward departure.

That was something that the United States, in this case the U.S. Attorney's Office with the District of New Jersey, decided not to do. You could make a strong argument that we should have done that, and you could tie that back to the atmosphere in the hacking community and the virus-writing community. It dates back to the "Morris" worm case.

I could tell you that one of the things I learned, in working on this case, was that people in these communities did not think they were going to get caught. And they looked at the "Morris worm" case and said, "Well, if I get caught, nothing is going to happen." And how does that permeate and affect behavior?

The second question is a good question: how do you calculate the exact damage? You can do that with reasonable estimates using statistics, economics. And it was actually interesting to try to put together a team of people who would have the right set of skills and knowledge and experience to make such an economic determination.

But it is very expensive and, to do it correctly, you have to do it worldwide, and that would only go to the monetary value of the property damaged, right? What about all the other related harm to society?

I don't know about you guys but, to me, it is pretty compelling when poor old grandma can't get her computer going for a week. And that happens to lots of grandmas, and that is very frustrating. That is a real cost to society, and I don't think that should be ignored.

Now it is not, obviously, as serious as the charitable group that needs e-mail to ensure that they know which elderly in their community need food. Because with the "Melissa" virus, these folks didn't get their food and certain things happened.

All these things could be thought of as the societal harm of these type of crimes. Do we want to go to the extent of figuring out where that plays in? I don't know.

MR. TRITAK: Could I ask you a question? You said before that you could have sought an upward adjustment. I think that was the term you used.

MR. TURRINI: Upward departure.

MR. TRITAK: Upward departure, and you chose not to. Was there any sort of public policy choice behind doing that, or was it more of a tactical decision? What was the reason?

MR. TURRINI: Well, the only way I can comment on that is I will give you my own personal opinion, not related to the U.S. Attorney's Office or the District of New Jersey or with the Department of Justice. If I were making the decision myself, I think it would be a very difficult thing to decide because it is such a new area of law. The whole basis of law enforcement is to control behavior. We want to facilitate behavior that is productive and dissuade and discourage behavior that we believe to be unproductive.

And there are many factors that go into how you do that. Should the Department of Justice have thrown the book at David Smith because we realized that there was tremendous societal damage and that we see future society damage? Maybe we saw that there was an element in this criminal community that needed an attitude adjustment, and that we could have used this as an individual case to adjust attitudes in this community.

Well, that is one way of looking at it. Another way of looking at it takes into consideration the individual defendant. Now, when he did this virus, did he know to 100 percent certainty how many millions of dollars of damage he was going to do?

What that illustrates is intention—what I find inherent in sentencing and not particularly well addressed in the guidelines is this tension between the defendant's subjective intentions and a sentence predominately based on economic loss.

So it is a very good question. It is a difficult one to answer. You can have strong arguments on either side as to how the Department of Justice should have gone and prosecuted the case.

MS. BANKER: Is there a question?

QUESTIONER: So that people can maybe put some concreteness on this question that she has asked you: how much time did Smith get pursuant to the plea?

MR. TURRINI: He has not yet been sentenced, but, if the judge were to accept the stipulations, he would receive a sentence between 46 and 57 months in prison.

QUESTIONER: Basically, between four and five years?

MR. TURRINI: Yes.

QUESTIONER: That is the sort of a concrete parameter—the decision that a sentence of four or five years is the appropriate sentence.

MS. BANKER: John, from your perspective, does that type of sentence sufficiently take into account the sort of societal harms connected to critical infrastructure assurance issues?

MR. TRITAK: Well, what was interesting in the comments that you were making is that you were taking into account a number of factors; none of them were the kinds of concerns I expressed.

I mean, one thing that sort of struck me is: what did he really intend to do, as opposed to what he actually accomplished doing, maybe even despite his efforts?

Let's turn it around a little bit. Suppose you got somebody who deliberately wanted to attack the electric power grid, with the only goal of giving Pepco a headache. But in doing so, he unintentionally caused a regional power outage.

Now there is clearly malicious intent behind what he was doing, *vis a vis* Pepco; and that is different from the sort of act exhibited during the denial of service attack where the perpetrator had no particular intent against any specific target or individual.

This is serious; but it is also more complicated. Let's say that the consequential loss and harms that flow from an attack without specific intent were considerably greater than anticipated by the attacker. It seems to me a sentence of four or five years would probably do a disservice to what he did and also, perhaps, send the wrong signal.

It seems to me that kind of behavior, that kind of activity, you want to strongly discourage. And, moreover, it isn't necessarily just a casual hacker who might try that. Suppose it is somebody who has got a slightly different set of motivations in mind.

It seems to me it is one thing to let loose a virus. It is another thing to deliberately attack and break in and actually destroy computer systems that can cause serious losses to major portions of the economy. I don't mean to suggest it is easy, but it seems to me I would be much more concerned if the guy walked way with a four-year sentence in that situation, than I do in the sort of calculations you were talking about.

First of all, let's say he is fairly new, and you know, there is a certain attitude in the hacker community that is not necessarily malicious in intent. It is reckless, perhaps, and irresponsible, but maybe it doesn't raise to the level of maliciousness. But the kind of thing I am talking about here regarding cyber attackers seeking to cause harm and serious disruption via the Internet, I think is a different kind of problem.

MR. DEMPSEY: I have a question. If a person intentionally lit a forest fire—and let's assume it is a federal forest—and, as a result, $500 million worth of timber were destroyed, but the person pled and agreed that the value of the timber was $80 million, would he then get that same sentence range?

MR. TURRINI: The way it would play out is there is a table of loss, it is 2B1.1, the property damage and theft guidelines, and the highest number is $80 million. So, if there is a case where the actual damage was over—

MR. DEMPSEY: That is what I am asking.

MR. TURRINI: —the actual damage was over $80 million, that is one factor that needs to be decided in applying the guidelines. So the parties can stipulate and say, "Well, it was over $80 million."

MR. DEMPSEY: I am just asking how is this different from burning down the forest?

MR. TURRINI: It is not. The only difference is that it is whether you can calculate either loss figure accurately. Now, I really know very little about forestry and forests, but I am assuming that you have got a number of trees and there is a dollar value per tree—not particularly difficult. Much more difficult to value the loss in the "Melissa" virus case because of the multitude of ways the virus infiltrated systems.

But, from a pure sentencing standpoint, it is not that different. The prosecutor in your case could decide, "You know what, this guy did so much damage, he intended to do $500 million of damage; he should go to jail 50 times more than someone who does—"

MR. DEMPSEY: Well, you put intent in there. Intent is different because the person clearly didn't intend to do one or the other.

John was sort of saying, "Well, what if you set in motion something; you light a fire, you want to just burn a cabin in a federal forest, and then it burns down the whole forest."

PROFESSOR O'NEILL: If I could just interject here because this is a little bit about what our last panel talked about. It is absolutely true that, in certain circumstances, we hold people liable, even criminally liable, for the reasonably foreseeable consequences of their actions.

Certainly, in the terms of like criminal conspiracies, if you are involved in a criminal conspiracy, you may not even know what some of your co-conspirators are doing. You can still be held criminally liable for their actions in furtherance of the overall conspiracy.

Now there are obviously doctrines that have developed over time in the common law that limit people's liability in a certain way. The difficulty in this particular area and one that the difficulties that the Sentencing Commission is grappling with, frankly, is that we know and have years of experience in knowing from Smokey the Bear that "you don't throw matches out in forests, they cause fires." Since we are assuming everybody knows that, we are going to hold everybody responsible for the reasonably foreseeable consequences of their untoward behavior.

The problem that we have in this context is that we don't have a long history of people letting loose computer viruses. The reason the $80 million figure is in the loss tables, frankly, is because generally it is hard to steal $80 million. And, until fairly recently, when you could steal a few dollars from a million different banks or you could hit these wide-ranging Internet conspiracies, it was tough to steal that kind of money.

So the thought that you were going to get more than $80 million, by golly, that is something else. It is still pretty hard now, but now the means to facilitate crime at that scope is much greater. It is just like the problem that we are dealing with concerning obscenity and pornographic pictures. You know, it used to be, "Well, yeah, okay, if you have got a dirty book or a dirty magazine, we are going to hit you. And, if you've

got a film, you know what, we are going to hit you for the videotape. But we are not going to hit you for every individual pornographic depiction that creates that film."

But, now, we've got the Internet problem and the problem of a file that can have a million photographs in a single file. How do we deal with that? The problem is we don't have a lot of experience in dealing with it.

MR. TRITAK: One of the things I was wrestling with in your comment was: at some point, if the losses are in the billions, you actually have a different kind of problem. I mean, it's not just in terms of magnitude of dollars and cents, but it is actually closer to something that requires a different kind of treatment because of what it suggests about the perpetrator and the potential societal harm that is implied in doing that kind of thing and creating that kind of economic loss. We are talking about activity that can harm the social and economic fabric of our country.

QUESTIONER: Let me just suggest something, and it would be a structural change, I think. Throughout this conference, not only here but at other times, people are talking about what somebody intended or what somebody didn't intend.

Well, you know, we have all sorts of instances where we deal with that. We have specific intent crimes. We have general intent crimes. Once in a while, when you are instructing your jury, you think, "Hmm, got to go and check to make sure this one is."

But, you know, we could structure this so that the prosecution would have the option of charging a specific intent crime which, obviously would be, number one, harder to prove and, number two, clearly carrying a heavier set of penalties under the guidelines; and we could have a general intent crime, and of course then they could be pleading down to them and so on.

But it seems to me, particularly in view of *Apprendi*, that we are going to have to maybe consider that. Because, at some point, particularly where you get into some of these mega-crimes and you have judicial determinations made, we are going to potentially run into *Apprendi* problems, particularly depending on how it gets flushed out by the various circuits.

MR. DEMPSEY: I am sorry, you were referring to what problems?

QUESTIONER: *Apprendi*. *Apprendi v. United States* is a case that came out, kind of the sleeper criminal law case of the term. But it observes, I think, broadly put, that fact questions are supposed to be decided by the jury. Now it has been interpreted to mean that, "Well, it is only in the event that it would enhance the sentence, and if you are within the basic sentence anyway, then it doesn't make any difference."

But you can get a lot of tinkering with that. And, not only that, when you are concerned about what I call the mega-crime—and let's not just look at $80 million; let's look at killing off half a state, somehow, or half a city—of course, when you have killing you have another story, but anyway—a specific intent and a general intent would be a tempting thing to go to and that may be something that might be necessary to go to in order to have appropriate levels of punishment.

MR. DEMPSEY: I have just two final thoughts. One is I was surprised to see that the top figure was $80 million. It struck me that that was a low figure given the way the economy is now, particularly in the context of computer crimes.

And the second deals with the problem of valuation—the fact that we know how to value trees more easily than we know how to value the damage caused by computer crime—still does not make a computer crime different because if you steal cattle or you improperly cut down trees and steal them from a federal forest, I think stealing one million dollars worth of cattle and one million dollars worth of trees gets you the same sentence.

And the fact that you have rules for both and we know how to value cattle and trees doesn't really make the crime different, and we will, I think, ultimately have rules for evaluating computer crime loss. But I also don't think that we try to factor in the loss of the peoples' vacations who couldn't go to the forest because it was burnt down.

QUESTIONER: Well, what about firefighters who get killed as a result?

MR. DEMPSEY: We do consider that. We may also include the cost to the government of fighting the fire. I don't know, but that would be another quantifiable cost.

MS. BANKER: Obviously, one of the questions is how much should go into the determination of loss. Viruses and the types of effect they have on companies is one issue. Denial of service is another. Then, the privacy violations that might go along with theft of credit card numbers or other types of hacking-type incidents.

One of the things you look at as an Internet company is: if something happens to you where you can't provide the services to your customers that they depend on you to provide or if you are not safeguarding information in a way that they expect you to, you sort of violate your relationship with your customers.

If there is a denial of service attack or there is a hacking incident, something like that, what is the way of measuring that loss of—let's call it good will—with your customer base for the victim company?

MR. DEMPSEY: But if there is a fire at a mall and the mall has to be shut down, do you factor into the loss calculation there for the crime of arson the lost revenue for the stores that did not suffer any fire damage at all, but simply had to be closed down for two days while the fire damage in the rest of the mall was being cleaned up? That is the same question. I don't know what the answer is on the arson side. But whatever it is, I think it helps us think about the answer on the computer crime side.

MR. TURRINI: Scott Charney talked about it in his earlier discussion. It comes right from the guidelines and I will quote it:

"In some cases, the monetary value of the property damaged or destroyed may not adequately reflect the extent of the harm caused."

And that is, I think, a very wise statement, and it allows a judge and a set of defense attorney, prosecutor in this judicial process to account for exactly what you are talking about.

MR. DEMPSEY: But I think if the sentencing guidelines are to mean anything, the decision has to be the same in the arson case as it is in the computer case. And if the mall is shut down in the arson case, then you would take into account the lost revenue and the inconvenience and the loss of good will and customer satisfaction, et cetera, of the stores who suffered zero physical damage.

MR. TURRINI: I agree—

MR. DEMPSEY: If it isn't done that way, then the fact that it was done with a computer should make no difference.

MR. TURRINI: I agree with part of what you are saying. You said that the guidelines would mean nothing if it weren't equal. I do not agree with that. But I do agree, and it is clear here, that this sentence applies to both types of cases, to all types of cases.

MR. DEMPSEY: Is it being applied to both kinds of cases?

MR. TURRINI: I do not know. What I can tell you, though, from my experience as a prosecutor, it all depends on the case, the defendant, the sympathies of the defendant, many different issues that go into whether the prosecutor wants to ask a judge to go upwards.

MR. DEMPSEY: I thought that is what the guidelines were supposed to avoid.

MR. TURRINI: It is a very rare occasion that prosecutors ask the judge to go up beyond what the guidelines call for.

We had a statistic yesterday talking about 0.6 percent of the cases in which there is an upward departure. I don't know what the percentage of cases is where the United States Government asks for it, but I know it is quite low.

Inherent in this entire system is the personality and the choices of the individual U.S. attorneys across the United States. One thing that probably is not readily apparent to the public is that the Department of Justice is not just one cohesive entity. Janet Reno is the Attorney General who is appointed by the President, but the President also appoints U.S. Attorneys in every federal district across the United States. Marty, how many U.S. attorneys are there?

MS. STANSELL-GAMM: 94.

MR. TURRINI: 94. And that individual U.S. Attorney, like in the "Melissa" virus case, has pretty much an autonomous way of choosing what happens in that case. Don't expect a comprehensive approach from every U.S. Attorney across the United States.

The thing I like about the guidelines is it gives a framework for the judges, in part, to try to measure cases against each other.

MR. DEMPSEY: That is why the judges don't like the guidelines—because they transfer discretion from the judges to the prosecutors who can make precisely the kind of discretionary and inconsistent

decisions that you are talking about. Then, when it gets to the judge, the judge is stuck with the rigidity of the guidelines.

MR. TURRINI: There is tremendous prosecutorial discretion built into the system.

MS. BANKER: Do I have a comment on the other side?

QUESTIONER: Yes, two quick thoughts. One thought is we are hearing that, even for those crimes where the loss can be monetized, it is very hard to figure out a monetary amount. We are hearing about lots of harms for which it is very hard to attach any kind of monetary measure, some of which seem very significant, some not.

We have heard a constant theme through these last two days that driving the penalties for economic crimes starting with or dominated by measuring harm may itself be sort of the wrong starting point, but that measurement of loss or gain is probably relevant in the end.

I would encourage the Commission and maybe the rest of us to think through a quick thought experiment. Could we imagine a penalty structure that didn't have a dollar calculation at all for harm; in other words, could we imagine other kinds of categories, other than accounting? And I think the answer is, "Of course we could." We have been talking about a lot of the kinds of factors or categories that would go into that calculation.

Then, we can back up and say, "Do we get to something that is more rational, that is more consistent, that is wiser, without taking a count of dollar values of harms at all, without trying to come up with a number, much less so many different categories?"

The answer there may be, "No, that dollar amounts tell us something, but we may be coming at it at the wrong stage in the calculation and in a far too refined fashion and not starting with a different set of categories of the kinds of harms that occur." And that list is not infinite. I hear of eight or ten different kinds of harms that seem to dominate lot of these cases.

Second quick point. Most criminal law professors, I think, would say, "We have no idea what you are talking about when you talk about specific and general intent," and the common law doesn't seem to have been a consistent category either.

However, if you talk about bringing *mens rea* in as another factor, there is a lot of commentary that has not affected Commission deliberations to date, including a number of cases by federal judges talking about how, "Isn't it odd that *mens rea* is what we teach lawyers, teach our students as this central defining principle of the criminal law. It is the basis for guilt. It is what distinguishes the criminal law, and then it is utterly ignored—the different mental states—in our punishment system, especially in the federal system?"

So we might think about bringing in those rough categories, the model penal code type categories—intent, knowledge, recklessness, negligence—in helping to sort out relative levels of punishment. And there is considerable literature that the Commission might, if it thought those sorts of divisions were relevant, consider, not only here, but for non-economic crimes as well.

MS. BANKER: Is there a comment in the front row?

QUESTIONER: Just one comment. Every time a federal judge instructs a jury, you have decided whether or not there is a specific or general intent.

MS. BANKER: The comment that was made was that federal judges, every time they are instructing a jury, do reach the issue of whether it is a general or specific intent crime.

QUESTIONER: Just one quick comment. One of the things that I heard this morning that I think is relevant to the loss determination, I think Scott Charney said it, is that the estimates from companies are often quite unreliable.

My sense is that, in these really large-scale cases where you have literally hundreds of thousands of victims, the estimates of loss are going to be more and more tenuous as time goes on. If that is the case, there is the other kind of more practical reality which is that I think judges, prosecutors, maybe even defense attorneys, really do not want the sentencing to become a separate trial.

I mean, the damage portion of civil trials is very often much lengthier than the causality determination. You could see that happening here. If that is the case, then maybe one possible solution is that loss may be one means to calculate, and that there is in a sense a whole separate structure for calculating those cases where loss is either more difficult to determine or where the calculation of loss is unreliable. But the choice is made. It is not that you have loss and then you add on specific offense characteristics.

And then, finally, the only other thing is I think any time you start tying specific offense characteristics to particular technology, whether it is encryption or any other type of technology, it is going to be obsolete in three years. Just like encryption now doesn't have the degree of sophistication that, perhaps, was what fueled that when it first became a specific offense characteristic. Thanks.

MS. BANKER: I'd be curious to know what the panel thinks about the idea of using factors other than just economic loss, sort of damage figures, for sentencing purposes.

MS. STANSELL-GAMM: I was intrigued by the idea of whether it would be possible to string this with a distinction between general and specific intent.

But, if you asked me—and Elliot, you might have some thoughts on this as well—what it is these guys, in fact, intend when they launch a virus or when they launch a DDOS attack or when they do some other very, very destructive thing? What is it they are thinking? Certainly they intend the act that is defined as criminal and so they meet the general intent gateway because the consequences then flow. They certainly have some level of *mens rea*, but I would probably describe it in the following way: "What I intend is to make a big splash and to shut things off and to make everybody notice me."

And sometimes the splash is bigger than they had in mind or it hits people that they don't have in mind. So they clearly intend some level of malevolent consequence, but it probably isn't very specific. It is probably not very directed, although, maybe in the DDOS cases, it is. It is probably very diffuse.

I would love to hear from Elizabeth or Howard how they think about this, coming from industry. But one of the things that occurs to me is I wonder whether it would be possible in sentencing not to try to quantify or describe the entire loss, but to just take some representative samples of different kinds of

consequences, understanding that this isn't the whole picture from which a judge could reasonably extrapolate. You know, just to give you some pixels of the image, but not all of it.

I don't know whether that would be a useful way of doing it or not. Because what Elliot was describing was a process, really, of statistical sampling. There was no way to catalog all of the damages from the "Melissa" virus. It just couldn't be done. So our solution was to spend the money to have a statistical instrument developed that would allow the people doing the statistical sampling to gather some information and then to draw some behaviorally sound extrapolations from that. I don't know whether that helps or not.

QUESTIONER: Frankly, all of that shows how crazy the guidelines, in some respects, are.

MS. STANSELL-GAMM: Okay.

QUESTIONER: When you have to do all of that in order to arrive at an appropriate sentence in a single case. I mean, that is nuts.

MS. STANSELL-GAMM: I don't disagree.

QUESTIONER: But you had to do it.

MS. BANKER: Did you have any comments you wanted to make in response to Marty's?

QUESTIONER: Thank you. A couple of things. One, as Elliot was talking about trying to quantify losses and everything for the "Melissa" case, I remembered getting calls from some of the folks in that case, from his office, and trying to do the same thing. As I think Marty and Jim both pointed out earlier, this is a learning process.

Not everybody at that point was prepared to sit there and say, "Okay, here is how many hours we put into the investigation. Here is how many hours for remediation. Here is how many hours we paid employees who were non-productive, et cetera." That was all a learning process. We came up with this figure, and it goes to risk management and there is that circle.

That is being done now, though. We are proactively looking at those things in the event of the next one that occurs.

The good news relative to that is the fact that that number has shrunken dramatically because we are better prepared. We are able to now stave it off in a matter of two hours as opposed to 48 hours we experienced initially.

The other thing relates to a culpable mental state, if you would, as far as what these guys are doing. I agree with Marty. I think a lot of the targeted companies weren't targeted for specific things, they were just targeted to cause that level of disruption, to make the splash to show, "I have been able to do this."

And it is very different from the physical side of it where those same individuals would be less likely to walk into this room and start slapping each one of us in the face, which would be extremely disruptive,

and, one having to physically extricate themselves from the room. They wouldn't do that, but they would do this electronically because there is that feeling that, "I am not really bothering anybody."

And I think that is a real difference in the way they think, and I think in the way we view them as a society.

MS. BANKER: Comment here?

QUESTIONER: But should we be looking at economics as the predictor of an individual's culpability, as to an individual's deterrence, or as to anyone's deterrence in any way whatsoever?

It seems like, from the first prior panel, the values seem to be the most important thing. And I want to add a few to them, not only the *mens rea* of being looked at, not only the intended harm, the foreseeability, but all of the other factors.

Was it the proximate cause? Was it something that was a "but for" cause? And, also, the conduct itself, the actual *actus reas*. Was the conduct itself of the nature that would have caused that harm in the first place?

You can't put economic losses to that. These are values you are dealing with. And I think it is important to consider that. Perhaps if the judges were provided with a structure of values and then judges could use the discretion with those values, as opposed to the prosecutors having that discretion.

MR. DEMPSEY: Some of these other factors are built into the computer crimes statute itself, and Marty is both officially and unofficially the world's leading expert on the statute.

But the statute itself draws distinctions between attacks on computers that are used for national security purposes, attacks on computers of the government, attacks on financial computers, theft of information from a computer, use of the computer, or the computer crime to extort.

And then you get down to what I think we are all talking about now which is only a sub-part of the crime. Each sub-part—(a)(1), (a)(2), (a)(3), (a)(4), (a)(5), (a)(6), (a)(7)—has a different sentence attached to it and has a different sentence for a second offense which is another value judgment, by the way. It is a value judgment across the board, but is particularly significant in the case of computer crime because of this sort of ethos, which is a wrong-headed ethos among the hacker community.

But when you get down to the viruses and hacker crimes, if you do a denial of service attack against a hospital, I think that is a significantly more serious crime. To a certain extent, not fully, that kind of thing is reflected in the structure, the substantive offenses of the crime. Maybe that is one way to think about it.

MS. STANSELL-GAMM: If I can respond to that. Title 18 U.S.C. § 1030 is one of the few sections that seems to use so many different provisions of the sentencing code. If you take something like mail fraud, you are sticking with one particular guidelines section. Where here, you have espionage, you have theft, and you have fraud—three different basic sections that you are going to be resorting to.

It seems like the structure of the criminality itself is probably the problem here. That's because the structure of the criminality is based upon the medium as opposed to upon what the actual crime is, the espionage crime, the fraud crime, or the theft crime. And if it had been structured correctly, perhaps we wouldn't have this particular problem.

But as long as it is structured that way, I think you do have to take into account the conduct, not only as to which sentencing provision applies, but the nature of the conduct once you turn to that particular sentencing provision.

MR. DEMPSEY: I was saying the opposite.

MS. STANSELL-GAMM: Well, actually the statute is strung kind of strangely. It has grown rapidly over time. The first pieces of it were passed in 1984, I think, and it was amended in '86 and then again in the early ‹90s, and then again in '96. So it has changed very rapidly, and I think what you see is the growth in Congress's understanding of the nature and scope of the crime.

Not just in the U.S., but in a lot of European countries also, the initial focus of computer crime was on fraud and theft. That is what everybody thought was going to happen, so they wanted to redefine traditional fraud and theft statutes in terms of computers to make sure that they were covered.

Then it occurred to everybody that there was also going to be damage to the computer and they came along later and covered that. And we have had several iterations of 1030(a)(5), which is the damage statute. The initial (a)(5), which is the damage statute, was strung in terms of whether you were an outsider or an insider. That was it. So what it did is it punished you if you were a hacker and you did damage. So the intentional act was the hacking; the damage was consequential.

People looked at the statute after the "Morris worm" case and said, "Gee, you know, maybe the intent of the actor should be factored in." So Congress threw out the old (a)(5) and created a new one. And what this one said is that it doesn't matter whether you are an insider or an outsider—which previously was the defining criterion. It doesn't matter which you are. If you intentionally cause damage, felony. If you recklessly cause damage, misdemeanor. That is it.

In the Computer Crime Section, we were concerned about the first version because, first of all, it didn't distinguish between levels of criminal intent, but also because it didn't criminalize insiders who intentionally cause damage. It just didn't capture that at all.

The problem with the second version was that it also overcriminalized and undercriminalized some things. The intentional damage was fine. That should apply equally to insiders and outsiders. But the reckless damage, it seemed to us, should apply, at least arguably, only to outsiders because you can imagine a situation where an authorized user has an on-beyond-stupid moment on the computer, does something really reckless and damages data.

Our view was, "Better be cautious about the imposition of the criminal sanction." That is likely (because you are talking about an authorized user) to be dealt with better administratively in some fashion. The other problem with the new statute is that it didn't criminalize hackers who negligently caused damage.

So, in other words, if we had a hacker who recklessly caused damage, if we were able to prove that the damage was reckless and not just negligent, we had a misdemeanor. So, what we said was, "Nope, you need both of those factors working together," and that is the structure of the current (a)(5). So what it says is: if you intentionally damage data, whether you are an insider or an outsider, felony. If you are a hacker and you recklessly damage data, felony. If you are a hacker and you simply cause damage, misdemeanor.

So that is the current structure of it. But, you are absolutely right. It has been an evolving process, and in fact, the current provisions point to even more different parts of the guidelines than you mentioned. They also point to the property damage provision and to the trespass provision. So there are lots of different values, and more than one of those can occur in a single case.

So, for example, in a hacking case, it is also clear that not only have you lost the availability of the network and the integrity of the network, but you have probably lost the confidentiality of it as well. So we have to look at every case and see which harms are present.

MS. BANKER: All right, great. Thank you to everyone.