Day Two—Plenary Session VIII

Sentencing Implications of 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*

Robert Chesnut, Esq., *Associate General Counsel, eBay, Inc.*

Kenneth Cohen, Esq., *Director of Legislative Affairs, U.S. Sentencing Commission*

David Green, Esq., *Principal Deputy Chief, Computer Crime and Intellectual Property Section U.S. Department of Justice*

John Reed Stark, Esq., *Chief, Office of Internet Enforcement, Division of Enforcement U.S. Securities and Exchange Commission*

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

PLENARY SESSION VIII:
SENTENCING IMPLICATIONS OF NEW TECHNOLOGY OFFENSES

PROFESSOR O'NEILL: I would like to welcome you all to the concluding panel of our Economic Crimes and New Technology Offenses Symposium.

I would like to provide brief introductions of the panelists who represent each of the breakout groups that met during our working lunch.

First, we have Elizabeth Banker, who is corporate counsel for Yahoo! I tried to refrain from asking her if she "Yahooed" today or not.

And John Reed Stark, who is chief of the Office of Internet Enforcement at the Securities and Exchange Commission.

Robert Chesnut, who is associate general counsel of eBay, from which I have bought everything from an old Captain Kirk poster to the watch that I am currently wearing, so I have some familiarity with eBay.

Then David Green, who is the principal deputy chief of the Justice Department's Computer Crime and Intellectual Property Section; soon to be moving off I am sure to be corporate or general counsel to some computer company out there somewhere, since that seems to be the trend that we have watched.

And then Kenneth Cohen, who works at the Sentencing Commission and serves as our chief congressional liaison.

We would like to focus specifically on what I think has been one of the more interesting topics that we have covered during the course of this day, and that is: is there anything different about Internet crime and cybercrime that makes it difficult to capture through the loss tables?

Does anything have to do with the criminal intent, the means by which cybercrime is committed? Are there things that need to be more appropriately or better captured by the sentencing guidelines that currently are not?

And then, of course, there are the loss issues. One of the difficult things that I think the Sentencing Commission has struggled with from the very beginning, and certainly we have struggled with a bit today, and that is how we define and decide loss in terms of cybercrime. Should intent have anything to do with loss?

We can start, perhaps, with Robert and work our way down, getting a report from each of our breakout sessions.

MR. CHESNUT: In our breakout session, we talked about mass media fraud and auction fraud. We talked a little bit about how the system is, in many ways, the same. The Internet is simply a new means to carry out the same schemes that we have seen in the pre-Internet days, although with a couple of key differences.

One is the power of the individual. You know, the Internet is just such a terrific tool, and it gives individuals a lot of information. But it also gives somebody sitting in a room an awful lot of power and can have quite an impact on the lives of other people in a negative way, in terms of bringing sites down and causing fraud and havoc in a number of people's lives across the country. The fraud can happen so quickly now, involving the Internet. In just the space of a few short days, the impact that one individual can have is really quite extraordinary.

There is some dispute and some difficulty in measuring how big a problem it is. In some cases, you might argue that it could be even under-reported because people are embarrassed about having lost money or they don't know how to report the fraud. In other instances, though, it is pretty clear that a lot of the auction fraud is actually over-reported.

You have a lot of people who are doing business directly with each other through the mails. And I know, at eBay, we see that the vast majority of the complaints we get resolve themselves when people realize that an item was lost in the mail or that they waited only seven days to get their item and they didn't realize that someone was holding their personal check for them. Or is it even fraud if there is a tiny crack in the back of a china plate where the description was, "It is in good condition."

I think we have a struggle in dealing with this problem, figuring out just how big it is and in measuring how serious the problem is. Even though the volume of complaints is high, the volume of business is tremendous. On our site alone, you are dealing with 4.5 million transactions in a single week. So there certainly is going to be friction, dealing person-to-person, and you are certainly going to have complaints that come out of that.

One of the real problems we see in auction fraud, in particular, is the dollar loss. You know, what we see are large numbers of victims, but not necessarily large dollar amounts. Over and over again—take the examples that we talked about, 80 to 90 victims, $30,000 in loss total among all the victims; this really raises some very challenging issues.

Where do these cases get prosecuted? Many cases along these lines won't meet the guidelines in individual U.S. Attorney offices. Yet, when you have got 75 victims spread out across the country or around the world, those are the sort of cases that local prosecutor offices really aren't well suited to handle because they don't have the resources to go out and find the victims and to deal with an Internet fraud scheme.

So that has been one of the challenges that we have looked at in this area, as well as the problem of juveniles. You know, over and over again, we see that a lot of these crimes are committed by individuals who aren't 18 years old. And there are a lot of aspects of the federal system that aren't well equipped to handle dealing with juvenile criminals. Yet, the juveniles are ones who are often committing the crimes, and they don't fully understand the consequences of their acts. They view it, perhaps, as an intellectual challenge or a game and they don't see or fully appreciate how what they are doing is criminal.

Responding to the challenge, a lot of it obviously falls on private industry to deal with. And you see a lot of companies—in dealing with mass media fraud and Internet fraud—coming through with escrow programs, identity programs, even insurance programs to help deal with the problem. That is an important part of the equation, no doubt.

But, also, dealing with the problem from a prosecution point of view and from the sentencing point of view has got to be part of it, and then getting the message across after people are sentenced. I mean, if these sentences are going to have any meaningful impact, the world has got to know about them. The world has got to know that you can go to jail for committing mass marketing fraud or you can go to jail for committing auction fraud.

I think there was certainly some debate in our group as to whether the current sentencing guidelines adequately addressed the problem. I think there is a lot of feeling that it did. There was also some sense that maybe it would be appropriate to look at an enhancement based on the number of victims, in addition to looking at pure dollar amounts.

If you have 80 victims who have lost $100,000, that is perhaps is a more serious crime than one victim who lost $100,000. You know, the impact is certainly a lot greater in society. It certainly creates a large number of challenges for law enforcement to deal with a large number of victims spread out all across the country. The impact is greater on the companies. A company like eBay, where we have 80 or 100 people who have lost money, there is certainly a greater impact than in the situation where there is simply only one.

So, perhaps we should consider some sort of a guideline, something in §2F, in the fraud table, that might recognize that a case where there are 100 victims or 200 victims, perhaps, is a more serious case than one where there is simply one.

And we also feel that there is a need to do something to address the problem with juveniles because we do see a large percentage of the crime being committed, in this area, by juveniles. That is our report.

PROFESSOR O'NEILL: Thank you.

MR. COHEN: Our breakout concerned intellectual property offenses and how new technology and the Internet has affected those offenses.

The most obvious change is that it has eliminated physical barriers. It creates large markets for infringing items. If somebody puts up an illegal copy of software to an illegal website, it instantly becomes available worldwide for anybody else to download. And not only that, the counterfeit item is an exact duplicate, a perfect quality match of the legitimate copy of the intellectual property.

It is easy to do. Anybody with a PC can do it. Another difficulty is that the victim often doesn't know that it is happening. Many people who were defrauded in the traditional context know that they have been swindled or, if an item has been stolen from them, they know that. But victims of this crime often don't know that they have been victimized.

We also heard a lot of frustration from industry representatives about the lack of enforcement for copyright offenses. Our data show, for instance, that last year there were 113 cases sentenced under the infringement guideline, and that includes trademark offenses which actually comprised the majority of those cases, we believe.

One of the reasons that we heard that not a lot of these cases are brought is because the guideline penalties were too low, until recently. In May, the Commission responded to directives contained in the No

Electronic Theft Act of 1997 by completely revamping the infringement guideline. We increased the base offense level from level six to level eight, and we changed the way that the economic harm is calculated in these offenses. In this Internet case, for instance, where we are talking about someone who uploads items to an illegal website, there would be an enhancement and a floor of a level 12, and the way that the loss would be calculated would be the number of infringing items multiplied by the retail value of the legitimate item. Whereas, before, it was the retail value of the counterfeit item.

That should substantially increase penalties for these Internet type of copyright infringements. We heard that that actually has kind of re-energized law enforcement and that they are actually responding to these; and that is having the intended effect that Congress wanted when it passed the NET Act, and that the Commission also wanted when it implemented the directive and revamped the guideline.

There really was a great deal of disagreement, however, on how you calculate the economic harm in these offenses. There was substantial disagreement, particularly in the Internet context, whether someone who downloads something from an Internet site illegally actually would have gone out and purchased the legitimate item; if not, there is no displaced sale of an illegitimate item caused by the infringement.

There also seemed to be some general dissatisfaction with loss being the only or primary driving force behind the sentencing calculations; something else needs to be prominently a part of it.

We didn't get as far as to say exactly what that should be, but the new guideline does do some of that; whereas, the old guideline didn't do any of it. We have an enhancement for manufacturing and importing and uploading to differentiate those offenders who put infringing material into the stream of commerce from those who are further down that pyramid. And we also have a downward adjustment for people who commit these offenses not for commercial purposes and not for private financial gain.

So, at least in this guideline, I think we have taken some initial steps toward making the economic harm calculation not just the sole driving force.

PROFESSOR O'NEILL: Thank you.

MR. GREEN: Our panel addressed the Economic Espionage Act which was passed in 1996 to address the theft of trade secrets. Interestingly, it fits uneasily but certainly within some of the issues that we have talked about.

It is not always a new technology offense. An insider can take a piece of paper that contains a formula, a key formula, and walk out of the building with it. It is not a new technology offense, but it is a way of stealing trade secrets. We also, of course, see the technology being more and more used to steal trade secrets that are held on computers or some other way.

Our feeling was, generally, that the sentencing guidelines work pretty well for people who steal Chevys. I go outside, my car isn't there, somebody else has taken it, they have gotten the worth of my car, and I no longer have my car. Even if they come and steal the car and they are caught immediately, the idea is they were going to get the worth of the car and they could be sentenced that way.

Thefts of trade secrets are much harder to value. There are a lot of different ways of valuing it, and Carla Mulhern, from Analysis Group Economics, talked about how trade secrets are valued in a civil

context and the 17 Georgia Pacific factors that you use to create a hypothetical situation where, if the person who had stolen it decided instead, "Gee, I wish to license it," and the victim decided that it would have liked to have licensed it, what number would they have agreed upon to license that property.

I think judges are fairly comfortable saying, "All right, we will use all those factors and award Company A $20 million. And, Company B, you stole the stuff and you pay $20 million." They are less comfortable saying, "Well, I don't really understand all these factors, but it comes out to $80 million, and we will put this person in jail for 323 months." There seems to be a real level of discomfort with that.

It is sometimes very hard to value this information. And one of the reasons is you can steal a trade secret from a company and it still has the trade secret, unlike the car. It is still producing. It may not even know for a while that it has been a victim.

If it is something like a formula or research and development, then it is also very hard to evaluate what exactly the defendant has gotten from that trade secret. Has it been able to make its product faster? Will it be able to cut down its research and development costs? All these are very speculative.

So, in these situations, courts in these cases—and there have been about 20 reported—there is a sense—and I am a little concerned about saying this in front of so many sentencing commissioners—that there are times when someone will look at the outcome number before they start looking at all the factors that go into that. I am sorry to break it to you.

Particularly this is the case where the numbers are so soft and judges can be so far all over the place. In a particular case that I prosecuted, we had a number that turned out very high or reasonably high, and the judge departed down 14 levels because of the over-involvement of the victim in the case, which was a departure we hadn't actually read about anywhere before and we are appealing that. Coincidentally enough, that worked out to a sentence of probation for the defendant.

So, everybody seemed dissatisfied with the way the current sentencing guidelines worked in the economic espionage cases. Sadly, we came up with many more criticisms than we did solutions.

One person, Joe Savage, was advocating looking at restitution as sort of a starting point; which is, what is the harm to the defendant and what amount of money should recompense that defendant for the harm that it or he or she suffered? And, from that, we should build on whatever the sentencing guideline is.

Again, we came across different cases, and the themes that have been echoed today came across in these cases. We have a case or some cases where the defendant is trying to steal very valuable trade secrets that could turn out to be a sting operation. While they think it is very valuable, in fact, it is worth nothing at all.

At other times, someone may stumble across—and we have had this kind of case—a new Intel chip. They were just trying to steal a computer; they got the brand new Intel chip, figured out what they wanted, tried to sell it for a few thousand dollars, and then found out what it, in fact, was worth, and the valuation was much, much higher. So that was a very high sentence in that case.

Again, I wish we could have come up with some good suggestions on how to fix it. There was a sense of real dissatisfaction that the sentencing guidelines have just not worked well with intangible property

that is clearly valuable, but where we may not be able to know with a reasonable degree of certainty just what the value is.

PROFESSOR O'NEILL: Thank you. Those are very interesting questions.

MR. STARK: We covered securities fraud and the Internet, and I really feel that we came to the conclusion very quickly that securities frauds on the Internet are really just the same scams, but with a different medium.

There are new issues, in terms of the ease and the efficiency and the inexpensive nature of perpetrating an Internet fraud. You can now manipulate the price of a company's stock without the use of any boiler rooms or bucket shops or offshore offerings or any sophisticated knowledge of the securities markets.

You all might be aware of the 15-year-old that the SEC sued just about a week or so ago. We have seen a lot of people like that who really have no knowledge or no understanding of the securities laws and how they work, who just decided to spread a whole bunch of false information about some companies to hopefully run up the price of the stock.

Is there anything different in the sentencing guidelines area? I am definitely not the expert here. I think it is a very tough task to calculate loss. Fortunately for us at the SEC, we really deal with the ill-gotten gains, and sometimes that is even a problem for us.

Is there really anything different, though, when these Internet cases present themselves to any of you all, when you are calculating loss? I think the answer to that is going to be "no." That is because securities fraud cases really—and particularly in regard to the Internet, when you are trying to figure out what type of damages were done—can be very tough on figuring out investor losses.

Some examples of recent losses include Emulex, where the SEC alleged that somebody spread a phony Internet wire release about Emulex saying that all these bad things were going to happen to it—its CEO was going to resign, the SEC was investigating, and it was going to miss its quarterly earnings target—and the market cap immediately dropped by $2.2 billion. And then, within just a few minutes after the NASDAQ suspended trading, it was back up to where it was. So how do you calculate losses there?

We brought a sweep. We bring these sweeps, occasionally, involving different types of cases. We brought one in which we alleged 16 different market manipulations, named maybe 30 or 40 different defendants, and we collected about $10 million in disgorgement. The SEC alleged that the market manipulation movement of all of those cases was somewhere around the $2 billion context. How do you calculate that?

One case we brought recently involved a company called NEI Web World, which is a shell company. The SEC alleged that a bunch of guys in their ‹20s on the West Coast spread some false information about NEI Web World over the Internet and managed to move the price, within 10 minutes, from eight cents to $15 and then back down again. Calculating loss there, I am sure, can be very tough. I guess you can probably try to figure out, using the NASDR, who the people are who sold and actually did get damaged by this. That is sometimes what we do in our disgorgement plans.

Another tough one is we brought an offerings sweep where we brought, I think, around 15 cases in which we alleged that fraudulent offerings were made over the Internet. Now those, in the private placement context and in your typical smaller offerings, you can usually find out who the victims are and who lost their money. Because of the Internet, you now can bring these cases before a single penny was raised. What happens in those instances where nobody suffers any losses?

Well, how can you bring a case when not a penny was raised? That does show you something that the Internet can do. The Internet provides this incredible window into developing fraud that we have never had before. I can log on, take a look at a fraud that is going on right now, analyze it, talk to my boss about it, and get to court to file a TRO pretty quickly when it comes to some of these offerings, because they are so fraudulent. And that allows us, sometimes, to get in there, believe it or not, before a single penny was lost, before you even have any complainant to even speak to.

I think those are cases that we are particularly proud of, and that goes to the idea that the Internet, in the area of securities fraud, these aren't hackers trying to tamper with the energy grid. These are people who want to be found. They spread their false information everywhere to a giant audience.

I am in that audience, personally, because I will go visit a site. It will use a cookie file to grab my domain, and then the next thing I know, I am receiving spam and junk mail from the fraud artist. Right now, I am conducting surveillance while I am sitting here, which is really pretty amazing.

So I think that, again, it has created this marvelous opportunity for law enforcement to really get in front of these cases and have this evidentiary trail.

The question came up in our discussion, also, when do the criminal folks get involved? Well, as I said, we brought somewhere around 200 or so cases in which the SEC alleges Internet fraud. I have been involved in just about every one of them, and every one of them, for us, can usually be—because the fraud is so outrageous—a bit of a marketing campaign as well, in that, we will provide the criminal prosecutors with the audit trails necessary, with a lot of the technical information, trading data.

All of the evidence that we have collected, with the proper request, we can provide to the criminal authorities, and we hope that you will take the cases. But you have got very tough decisions to make on your own side, in light of resources. And, perhaps, cases or people in our discussion group aren't necessarily worthy of criminal prosecution, and that is why we have the SEC as kind of a quasi-law enforcement agency to bring these cases.

So those questions, I think, are getting better and better. More and more criminal prosecutors are interested in our cases. Of those 200, maybe 30 or so were brought criminally, and just about every one of those involved some type of fraud charge.

But I think the bottom line is there is no standard composite or profile for the Internet scam artist. There is no way. Of these 200 cases, every single one of them is different, and it involves a lot of judgment calls along the way.

The only thing that I can say for sure is that most of them—although it is easier, faster, and cheaper to conduct these Internet frauds— present, I think, the same ideas of loss and some of the same problems

that traditional securities fraud cases presented, which, it seems to me, are fairly significant based on the discussion of the criminal prosecutors in the group.

MS. BANKER: My panel was primarily discussing crimes related to distributed denial of service attacks, viruses, and privacy violations that may come from hacking.

Even though those are much different types of crimes than a lot of the ones that have been discussed by the other panelists, I think a lot of the themes are the same, focusing on the difficulties of coming up with a dollar value that represents the loss that was sustained by the victim or victims in a lot of these cases, and using that as a basis for sentencing and the types of results that you see.

One question that is obviously raised is whether, after coming up with the dollar figure, if the resulting sentence actually does capture sort of the seriousness of the offense, is whether it is a sufficient deterrent and what it communicates to the sort of community-at-large that participates in those types of activities.

That is one of the real challenges involving the types of crimes we were talking about, the denial of service, the viruses, those types of things because you are talking about a community of people who engage in those acts. Many of them are juveniles, but many of them also don't necessarily do it for the sake of making money off of a fraud scheme or anything of that nature. It is more about gaining notoriety. It is a challenge. It is fun. It is pointing out security flaws in other people's systems for them as a public service, you know, however you want to put it.

The other side of that is that because they aren't doing these acts with a specific aim that is really reflective of the types of damages that are caused, they may not be going into it with an intent to cause the amount of damage that ends up being the real consequence.

One of the things that the group talked about is how to take into account the intent. Should it be important whether somebody is reckless or whether the intent actually is to take down the power grid or something like that that is truly malicious?

One of the other things that we talked about was just the difficulty of coming up with the number value, actually making it dollars. And some of the challenges that came up in that context were: the difficulty of getting accurate, useful information from victim companies; the lack of experience that we have in dealing with things like large-scale viruses; and the history of the computer crime statutes and the fact that they grew out of fraud activities and things where there may be a theft of something of value.

But, what about the denial of service situation or a virus situation where the result is that users who could be anywhere using the system for virtually anything? One example that was given was the charitable organization that delivers meals to elderly people. Do they know where the need is and are they going to be able to get the food there; are they deprived of that? And wide-ranging societal harms that could actually result from these types of activities.

The group actually was entertaining the idea of putting aside the effort of trying to come up with that dollar figure, looking at a wider range of types of harms caused from acts, and using that as some way of focusing on what the sentence should be. The types of harms include everything from privacy violations, the compromise of somebody's medical records, loss of use of a system for business purposes, lost

customers and those types of more consequential type damages, and then the loss of crucial services, whether they are hospitals or electric power, those types of things.

PROFESSOR O'NEILL: Thank you, Elizabeth. Before I turn the time over to see if we have any questions, I would like to ask the panelists to comment on three different questions. We, in part, have talked about them before.

First of all, was it the majority view in your individual breakout group that there is a real difference between cybercrime and other types of crime? Is it a difference in kind, or is it simply a difference in the means, using the Internet or a computer as an instrument?

Secondly, whether or not—setting aside the complicated issues of calculating loss or gain or whether gain should even be considered, and that is "whether or not" in these types of crimes because they may be somewhat different or at least the scope of them—the potential impact of the crime may be different from a crime committed in real space.

Is it more important that we focus at or look at *mens rea*? And is there a place for differentiating between specific and general intent crimes and bringing in the idea of *mens rea* and intent back into the sentencing equation, which it is largely left out under the current sentencing guidelines?

And then, finally, it is generally understood that the sentencing guidelines, in part, were a creation that was based upon prior sentencing practices of judges. And that, in fact, was an important gauge for looking at how society and how judges valued different and specific crimes. Is there any value to waiting and allowing this particular area or these particular types of crimes to percolate out there in the field, to see what, in fact, it is that judges do and how they treat these crimes and to allow us to have information that we can then build upon perhaps in crafting guidelines, truly guidelines in the future? Or is the problem so sufficiently severe that it is important that we act now and plug up potential holes?

I would just be interested in sitting back and seeing if anyone has comments or a sort of group feeling about those issues.

MR. GREEN: I would address the copyright guideline, which the Justice Department worked on, and we really appreciated a lot of the very hard work that the Sentencing Commission did to try to come up with a right balance on a very difficult issue.

I know Ken put a lot of work into that and Vicki Portney, from our side, and a lot of people tried to come up with something right.

I think that is a good example of why you can't wait, and it may be instructive for other areas as well in that I think the guideline was broken, in part, and based upon something that didn't make a lot of sense. And judges, and I think members of the public, did not treat intellectual property crime as a real crime, so they would look to drive down the numbers to either depart downward or did not really sentence people—particularly in copyright kind of crimes—to jail, with the feeling that, "Hey, this isn't really a criminal. This isn't really conduct that we really disapprove of."

And that was problematic, in part, because the Justice Department was now less likely to make that kind of effort—that is, bring a criminal case—if that was going to be the result, with the further result that

we didn't have deterrence. We didn't have an attitude that this was going to be something that you shouldn't be engaged in.

I think in that way, certainly with a strong push in the back from Congress, the Commission said, "Hey, wait a minute, we have to change the sentencing guideline and look at this in order to change the Justice Department's conduct to make sure that they bring more cases, to change the criminal's conduct by letting them know that this is real crime, and to let the judges know that this is real crime and they need to start treating it that way."

So I think in some of these cases, we can't let the market lead. We have to say, "Wait a minute. We have to come up with factors that are proportionate. We need to understand what the hacking kind of cases are going to bring and the damage that they can come up with, and we need to come up with factors that address that, without letting a lot of time pass and a lot of damage be done.

So I think the Commission really has to be more proactive than reactive in this area.

PROFESSOR O'NEILL: David, would you say that the problem is either that judges aren't doing an adequate job of understanding and sentencing these crimes appropriately or that perhaps there isn't a sufficient incentive for prosecutors to actually go out and expend scarce resources in investigating and prosecuting these crimes?

MR. GREEN: We find crimes where there may be a relatively small amount of damage and so prosecutors are unlikely to bring those cases because the person won't be prosecuted.

In turn, companies are often unlikely to report those cases for a lot of reasons, but one is, "Hey, we don't see many prosecutions." So what may look like a single incident involving a single company that is not worth very much, may actually be a lot of companies being hit by a particular defendant, but nobody is reporting it so we really may not realize the scope of that.

We were working at the law enforcement end to say to law enforcement and prosecutors, "Hey, we have to take those cases. We have to take even the smaller cases in order to create some deterrent effect and to encourage companies to report." But, oftentimes, we get the attitude on behalf of the public and on behalf of judges that "these are just kids having fun and we are taking this way too seriously," and it is discouraging.

MR. STARK: With respect to the Internet fraud, as I said before, it is just a different means. They are the same old violations. I predict that just about every SEC case, within a couple of years, is going to be an Internet case and will involve some component on the Internet. It is slowly creeping that way.

Which begs the bigger question, "What am I going to do for a living after that? Because I have developed a specialty that I think is diminishing because so many people understand and use the Internet."

But there is an incredible culture of vigilance on the Internet. If you go out on a message board or send a spam or do something, we get about 400 e-mails every day from people reporting suspicious conduct to us. It is rarely a victim e-mailing us to say that he or she has lost money. It is almost always someone who says, "I saw this and I want you to do something about it."

In some of the fraud cases where someone posts a false or fake earnings release or fake announcements on a message board, within a few minutes, people are responding, saying, "The SEC is going to arrest you." Now, as you all know, we don't have arrest authority at the SEC, but that is how vigilant they are. There are message boards dedicated just to alerting the SEC of problems.

So the deterrent effect of one decision is really incalculable it because every time we bring one of these sweeps, it bumps up our average number of e-mails every single day, every time we bring these cases.

It is almost impossible for me to sell a case to a criminal prosecutor when not a penny has been raised on a case—if no investors lost. But the irony of that, to me, is that those are the most important cases that we bring because we have brought them before there is any blood on the floor. I am most proud of those cases because we stopped someone before they ripped off somebody.

They are not going to make the headlines, either. That is the reality of a case where no money was raised. Everybody always wants to know when you bring one of these cases, "Well, how much money was raised? How much money was lost?" And I don't really think that that is a measure of how serious the securities violation or, in many cases, the fraud, the crime is.

There are cases where you are just dealing with a prankster. You have tremendous discretion, I think, in your own prosecutorial agency to decide that this is just a prankster. This isn't someone who really knew what they were doing.

In our situation, at the SEC, we are not as sympathetic to pranksters as a lot of criminal prosecutors are because we don't have the same level of intent that is required for the types of cases that we bring.

Well, we brought a whole bunch of cases that I think some criminal prosecutors have declined, but they are glad that we are here to bring the case so that they can feel that something was done.

Should we let this stuff percolate and see how it turns out? Obviously not. We have been very proactive at the SEC, at a very, very early time, to make it known that we are on the Internet. We are going to be aggressive when it comes to securities violations.

In my view, it is really just a small group of people on the Internet trying to spoil it for the rest of us, in the area of securities fraud. And I think they know that we are out there and that is a huge thing. That is why we have to keep bringing cases as much as we can because you want people to feel like the bad guys are being taken off.

And that is another very difficult task for us because if we do too good a job—and you see this in the message boards—people say, "Oh, this is okay, the SEC is policing this pretty well, so you really don't have to worry. You can believe law enforcement nowadays. All the crooks are off."

So, if we do too good a job, we are in trouble because then investors start relying on people. If we don't do a good enough job, then the crooks take advantage of people and steal from them. So you are never going to win in that situation. You are just going to do the best you can by bringing as many cases as you can.

But, as I said before, the crimes are much easier to commit, given the Internet. You can do it from your living room. You can commit a very, very effective securities fraud from your own living room at no cost with virtually no expertise in the markets. The reality, though, is the violation that you are bringing or the fraud that you are perpetrating is the same type of fraud that has really plagued the markets for centuries.

MR. COHEN: I would like to respond to some comments that David mentioned on whether we should wait and let things percolate. Well, in the area of intellectual property, the Commission obviously didn't have that luxury. Congress gave this new Commission 120 days to promulgate a new guideline.

However, the Commission should—and I am sure will—monitor the operation of the new guideline over time and see how well we responded to the problems that Congress identified under the NET Act.

But there is one issue that was raised in our breakout session that I think responds to some comments that Dave had mentioned. It is that we may have created a problem in the new guideline because some of the offenders who most likely may be deterred by sentences other than imprisonment, now, more likely, will get imprisonment. Take, for instance, the college student who is uploading infringing material, not for profit or commercial advantage, just because he can, just for the sport of it.

Some believe that a few well-publicized prosecutions of that kind of behavior would have a very wide deterrent effect among that segment of offenders. But, now, we have a guideline for those offenders where probation, for instance, may be most appropriate. And this is all subject to argument, but those offenders start off effectively with a level 12.

And now, every time that someone downloads an item from that illegal website, that will be valued at the retail value of the legitimate item multiplied by the number of times it was hit. You could potentially see some very high sentences there. And so that kind of goes also to Mike's question about intent, and it seems like some people who don't have the worst intent may get some of the heaviest punishment.

PROFESSOR O'NEILL: But is that appropriate? Do you or did the group think that?

MR. COHEN: I did not get the impression from the group—and others in the group can disagree—that they thought that necessarily was appropriate. In fact, our discussion kind of got away from whether intellectual property, copyright infringement, over the Internet is different—or new—from traditional infringement, rather than actually comparing it to just fraud in general. The Commission took an approach to try and bring the guideline for a copyright infringement much more in line and make it look a lot more like the fraud guideline.

And many in the audience thought that, "Well, maybe that was mistaken," because not everyone is going and stealing new Mercedes Benzes, but everyone is infringing copyright; and, therefore, the public obviously doesn't feel that they are quite the same.

MR. CHESNUT: I want to comment on something John said. I think in the securities area, he is right; it is the same crime, just a new way of doing it.

That may not be true, though, of all the stuff we are talking about today. The denial of service attacks are something eBay has had to deal with. That is all new. There has never been, I don't think, a

similar crime in the offline world, and it raises some really interesting issues as to how you would calculate loss.

For a company like eBay, undergoing a denial of service attack, there is certainly a cost to eBay, but there is also a tremendous cost to the people who depend on our service to make a living. And, when our site is down, there are a lot of people who can't make their living because they can't even get onto our site. Then, of course, you have got the cost to our stockholders because our stock price goes down the next day because we were a victim of a denial of service attack.

And I have even heard a suggestion that—since a lot of dot.coms lose money—if you knock one of these guys out for a day, maybe the defendant should get a credit for the amount of money he saved the dot.com by being down a day. I don't know.

MS. BANKER: Actually, I am not sure that my panel agreed on whether or not computer-type crimes, the denial of service, are really that different from more traditional crimes. Obviously, you can put any business out of service—an electric power company—with a well-placed bomb. So there is some precedent for that.

I think most of us probably did agree that there were some differences between the computer crimes and the more traditional ways of achieving them—whether it is fraud or something of that nature. They are difficult to investigate and they are difficult to prosecute because of the challenges in the legal framework, it is not necessarily where it needs to be. There are global issues, in terms of jurisdiction that are very challenging. I mean, there are a lot of things that really do make computer crimes very challenging to deal with.

I don't think we identified any factors, though, that we thought should be considerations for sentencing. So I guess that is how I would respond on that issue.

I think intent was very important to the group, though, because there is such a wide range of potentially bad actors and of potential results in the computer arena—whether it is simple webpage vandalism or hacking; theft of credit cards or other data that might be stored on systems; interrupting services; something like Yahoo! where people are looking at what their stock price is; or things that may be more critical, financial services; maybe they are actually trading the stocks not just looking at them or doing other financial transactions—you know, the critical infrastructures that really rely on networks to deliver services.

And then, there is the whole other category of information warfare. So there is this huge range. And, if you don't take into account the intent at sentencing, if you just look at the results, the sentences may be unfair.

PROFESSOR O'NEILL: Is that a problem, though, of the crime of conviction in determining intent in the type of substantive offense for which they are prosecuted, or does that go ultimately to the sentencing decision?

MS. BANKER: I think most of those types of crimes are going to be prosecuted under section 1030, to some extent, and maybe somebody who does prosecute those would have something to say about it. But, you know, there are different levels under 1030. I mean, it makes a difference whether it is a

national security computer system. It makes a difference whether they are financial records, that type of thing.

But just because you may have picked a target system—maybe that just shouldn't be necessarily the sole deciding factor in the severity of the sentence.

MR. GREEN: Even in the example you gave, it shows some of the difficulties. With Yahoo! for example, someone might say, "Well, those people couldn't check their stocks for a few hours." I think probably some of the people at Yahoo! would say, "Well, wait, that is even more important than that."

But there are other people who may either now or in the future have their calendars on Yahoo!, and now have to do the next thing. They have relied on Yahoo! being available and now can't do that. And I know we are getting into sort of consequential losses, but trying to figure out how much economic harm there was and how you measure inconvenience from a denial of service attack is extremely difficult, and there are lots of ways to do it.

People were talking this morning on eBay. Well, it was down for a couple of hours, so people waited and did their shopping later on. And you could argue that they went to some other site that was available and got their goods there or that they found it frustrating and said, "Gee, this is the one time I wanted to get on eBay, now I am not going to get on eBay anymore."

And, of course, all this stuff is really hard to measure. But, even though it is hard to measure, it doesn't mean the consequences aren't out there.

MS. BANKER: I think with the Internet that one of the things that is particularly hard to deal with is every time there is a denial of service attack or a hacking attack where, let's say, somebody gets credit card numbers of people who have bought stuff online, we are at a stage where we are still convincing people that they should be willing to do e-commerce online.

And, every time something like that happens and is publicized, it takes us back a few steps. So it really hurts the entire industry, and I don't think there is really any way to calculate that.

MR. STARK: I think some of this relates a little to what a lot of my students say. I teach a course, Securities Law and the Internet. Take a case like this kid that we sued, this 15-year-old. His name is Jonathan Lebed. He spread false information about 11 different stocks, and he profited considerably by spreading that false information. He spread it about a lot of thinly-traded companies.

And the reality of it is that a lot of the people who took his recommendations, or take any of these recommendations, act on this quickly; they are, in my opinion, not very smart investors. Investors should be doing their homework, should be making a calculated and careful decision when they make their investments.

But there are a lot of investors out there who are gamblers. There are even investors out there who are looking for good crooks who are spreading false information. For them, it is a gamble. So why should the Commission or the SEC or a criminal prosecutor protect those people? Why should they even bother?

The reality, though, is that that is never going to factor into our analysis, in my opinion. There are always investors who are new. There are always investors who can be lulled in. Just think of yourself walking into a store in Georgetown. You do not have not a lot of money because we all work in government. You walk in, you don't want to make a purchase. You have no desire; you have no need for anything. You walk out, and you have just spent a big chunk of change on something that you probably should return.

Well, why did you do that? Well, there was a good salesperson in there. And everyone has experienced that at one time or another. So I am always going to feel some sympathy for investors, even the ones who are gambling because people don't know a lot about gambling. So, if I am going to look at the victims and how much they have been harmed—some of my students would say, "Well, you should just ignore them; they are all just a bunch of greedy people anyway"—I don't think you should do that. I, personally, don't think that our program should factor in such things, but I think others disagree.

PROFESSOR O'NEILL: I would like now to open it up to the floor for any people who may want to add to what one of their panelists that represented their groups had to say or if anyone has any questions or comments before we come to the close of this meeting.

QUESTIONER: With regard to the question you asked the whole panel on whether or not—with regard to these particular crimes as compared to others—the question of intent becomes more important than it might be in other fields, I merely want to stress that in the regular teaching and learning of criminal law, we learn very early that in the Anglo-American system we do not look into motive, we look only into intent.

There are hardly any crimes where motive is considered. Motive became very prominent in a new crime, which is the hate crime. And the question that I really is: is this an area where issues of motive will become sufficiently important so that we need to consider whether or not in criminal law dwelling completely on intent alone is sufficient?

PROFESSOR O'NEILL: That is a very good question.

MR. STARK: At the SEC, we have got to consider the integrity of the marketplace. We are here to make these markets the best in the world and keep them the best in the world.

And whether you are a prankster or a scam artist, if you disturb the natural flow of that market, we are going to take action. And I think that is the appropriate way to go. So, just because somebody thinks it is fun and funny to manipulate the price of a stock—even if, again, no investors lose any money or maybe it is false information being spread without necessarily any significant impact on the price—I still think it is something that we need to act on.

We are always going to be looking at something like materiality in the context of whether or not the violation takes place. But, as I said, we don't really differentiate too much between the prankster and the scam artist. And I know that they are different people, but the impact on the marketplace is something that we have to protect either way.

MR. GREEN: And, in the criminal law, under Section 1030, for example, 1030(a)(5), we look at whether there is an intent to cause harm, which would be a felony, or was reckless, which is also a felony,

or whether the person intended to go into the system—didn't intend to cause harm but, on the way out of the system, knocked some things off with their elbow that ended up putting the system down—speaking metaphorically.

So those are questions, to me, that blend motive and intent. But, certainly, whether someone was trying to cause harm or was acting without regard or was not really trying to cause harm but still being somewhere that they ought not be changes the character of the case under law as well as characterizes the way the prosecutor looks at them. And I think that is appropriate.

PROFESSOR O'NEILL: I would also add that it is easy to conflate motive and intent. And, as you know, those things are very closely aligned. But I think you make a good point.

Like in hate crime, which has been sort of the rage most recently, in being able to enhance sentences, for example, based upon racial animus, whatever motivations that people may have. That is sort of an interesting way of looking at this area of the law as well: and how not only intent is affected. Oftentimes in the criminal law, of course, we assume it, from the *actus reus*, the *mens rea*. From the very act, you assume the intent.

But that still is a difference and perhaps it is a difference that makes a difference as to what the motivation of the crime may be. Are there any other questions?

QUESTIONER: This is actually a comment and a question. In terms of the issue of intent, it seems to me that for sentencing purposes, if you are talking about intent, you have probably already lost the argument. And now, in terms of how it impacts at sentencing, it likely would be an enhancement, but probably otherwise has already been washed away in the trial or the resolution of the case by plea.

In terms of cybercrime, we have tended to focus on §2F, how the fraud guidelines interact, and whether the guidelines generally are sufficient to deal with the phenomena of these new crimes.

I am wondering if any of the panelists see other provisions—money laundering, for example—as more readily available in certain aspects of cybercrime, such that what may be viewed as a deficiency in the §2F guidelines for penalizing certain conduct to the level that some of you may want, might not be picked up in the charging decisions that prosecutors are making.

PROFESSOR O'NEILL: I am always a little bit concerned about packing too much into a particular provision. I think one of the perfect examples of that is acceptance of responsibility. There are so few downward departures that are permitted, that we have seen case law develop over time that packs a lot of things that aren't really classic acceptance of responsibility into the acceptance of responsibility downward departure guideline.

Now, maybe that is a good thing, in that there may be things that we ought to kind of mask in terms of what we are allowing downward departures for. We don't want it to be made explicit. That is certainly a possibility within the system. But it also becomes a bit difficult to facially support packing too much into provisions where the fit, perhaps, isn't quite as neat.

MS. STANSELL-GAMM: We were talking, in our breakout group, a little bit about the development of the Computer Crime Statute and where all the various pieces of it point in the guidelines.

And you are quite right that, initially, when the Computer Crimes Statute was passed, it was tied to §2F1.1, the fraud guideline, and the fraud pieces of it still are, you know, § 1030(a)(4), which is a fraud statute, but other pieces of it point to other guidelines.

So, for example, the damage provision that we would use to prosecute the distributed denial of service attacks, points to the property damage guideline so that we have pointers to §§2B1.1, 2B1.3, the trespass guideline.

The first one, for example, points to the espionage guideline. There is a computer extortion provision in section 1030 that points to the extortion guideline. So, actually, those sign posts are going in all directions, and I think as some people noted in our breakout, it displays a little bit of the disintegration of the statute.

But, I think the Sentencing Commission has, without creating a separate guideline for the Computer Crimes Statute, done the best it can within the existing structure to point the various pieces toward the values already existing in the guidelines that best match. So that is what we have got to work with right now.

QUESTIONER: I think it is true that a lot of the cybercrimes go to different places. But I am willing to bet that most of them end up back at some sort of quantity-driven table, whether it is in §2F1.1 or one of the referring guidelines.

And yesterday, we heard a lot about how difficult it is to define loss, first of all, and then to calculate it in some kinds of cases. It seems to me, today, that we have heard a lot more about how difficult it is to calculate—loss in cybercrime in particular—and how it might be—even if we could come to a figure most people would agree upon—inappropriate to use that as a basis, maybe because of the vast disparity between the intended harm and the actual resulting harm, and so on.

I am wondering what the panel thinks of the idea of using—as a starting point for the punishment of cybercrime in particular—something other than a quantity-driven monetary table, and if so, what sort of factors you might use instead.

MR. CHESNUT: I guess, in our panel, one of the things we kicked around was the number of victims as at least a factor in it, as opposed to simply a pure financially driven situation. I think there is something worse. We see it in the auction fraud area. I think if you have 100 people who each lose $1,000, that is worse than one person losing $100,000. And the number of people involved, I think, is certainly a factor that isn't considered adequately under the current system.

MR. GREEN: I think some idea of loss still does properly stand for how bad a crime it is. I still think that it makes some sense to punish someone who creates $80 million worth of damage, like in the "Melissa" virus, more than someone who creates something that doesn't do very much damage at all.

But I certainly agree that that can only be one of the factors. And if we are relying so heavily on loss, then we tend to put a lot of things into loss that loss can't really bear, and the guidelines don't work very well.

MS. BANKER: I think that is basically the way the group that was talking about denial of service and viruses looked at it. I don't think anyone was really recommending that you just completely discount the dollar values on damages. But recognizing things like coming up with an $80 million figure for something like the "Melissa" virus is an incredibly difficult thing to do. It is my understanding that that is where the guidelines tap out, and that has a lot to do with that dollar figure; and there may actually be higher numbers out there for damage.

You wouldn't necessarily want the sentencing process to just focus on how you come to that number and have that be the only factor in sentencing. Maybe there isn't necessarily a need to associate a dollar amount or somehow quantify those harms as long as you recognize that these are the types of harms that were caused by this action and use that as sort of a real starting point or at least a departure point for sentencing.

PROFESSOR O'NEILL: We have time for one final question before we end the meeting, and I see a hand right over here.

MS. STANSELL-GAMM: I was just going to make a comment on the last discussion. I didn't mean to say, at all, that I think that the economic loss tables, whether they are found in the fraud guideline or the property damage guideline, are where the discussion ought to center.

I think one of the things we all agree on is that, while loss is a huge component, it is hardly the only one. And, right now, it is the driving force. The other considerations that we have talked about that are so important—privacy and public health and safety and restoring the confidence of the network or the confidence of the customers in the network—are departures, which I understand yesterday you looked at. And judges are departing from the guidelines in a very, very small percentage of cases.

What that tells me is that the economic factor is really driving the sentencing, and I am hardly speaking for the Department of Justice, but it seems to me that that is not the right result, that other things—some of these intangibles—need to factor in at least as heavily as economic loss.

PROFESSOR O'NEILL: Well, thank you. Before I turn the time over to Judge Murphy who will be delivering our closing comments and adjourning this meeting, I would just like to thank the panel for all the useful comments that we have received and offer them a hand for the work that they have done.

Since I teach criminal law, in this classroom on occasion, I would just like to give each of you an assignment before we leave, some take-home work to be thinking about. I guess the collective wisdom of the group is always better than the wisdom of the individual.

Basically, among the things that I would like you to think about—as you go back to court or go back to prosecuting people or go back to your companies and think about these issues—is basically how we raise the costs of cybercrime in terms of having the guidelines in sentencing be a deterrent.

How can we use the sentencing guidelines as a means of informing people of the problem of crime and informing and shaping their preferences? And, also, do we currently have a sufficient base of knowledge from which to draw adequate guidelines in this new highly technical area? Although it has a lot of similarities to crime in real space—and, frankly, I think Easterbrook was probably right in the idea that there is no real need for the law of the horse—there are differences in the means used to facilitate crimes.

So do we have a sufficient knowledge of crime out there and the way that crime has functioned in the cyber-world to adopt new guidelines in this area?

And then, finally, should *mens rea*—whether you characterize that as intent or whether we also concern ourselves with motive—have a larger role to play in fashioning guidelines for the future, especially in this particular area? Thank you.