Day Two—Plenary Session VI

Applying the Guidelines to New Technology Offenses

David Goldstone, Esq., *Head, Intellectual Property Rights Team, Computer Crimes and Intellectual Property Section, U.S. Department of Justice*

PLENARY SESSION VI:
APPLYING THE GUIDELINES TO NEW TECHNOLOGY OFFENSES

PROFESSOR O'NEILL: David Goldstone is a trial attorney in the Computer Crime and Intellectual Property Section of the Criminal Division of the Department of Justice. There, he is currently the co-chair of the Justice Department's Electronic Commerce Working Group. He has been active in developing Department policy in many areas of electronic commerce, particularly related to legal and litigation issues relating to use of electronic translations. I would like to just take a moment and offer a hand to and give our thanks to Mr. Goldstone for his willingness to participate in today's discussion.

MR. GOLDSTONE: Thank you. It is a pleasure to be here today. Before I get into the substance of my presentation, I would like to talk about what we are doing here today, talking about new technology offenses. I am reminded of a conference that was held at the University of Chicago four years ago in 1996. The keynote speaker there was Seventh Circuit Judge Frank Easterbrook.

He came, as the keynote speaker, and said, "Focusing on law of cyberspace is as useful an inquiry as focusing on the law of the horse. We shouldn't look at special cyberspace issues; instead, we should look at general principles. And, from these general principles, we can learn how to apply the specific cases."

I am not going to disagree with Judge Easterbrook, but I do think that there is value in looking at new technologies and the ways in which, particularly, crime has changed across a broad spectrum of areas. You just heard presentations about fraud and about computer hacking, but there are many other areas as well.

And the sentencing guidelines have recognized many of these changes over the past few years. There have been many updates; more in some areas than in other areas. I hope it will be helpful to you to consider a few different kinds of new technology offenses and to compare and contrast how the sentencing guidelines do or don't recognize the way that cyberspace has changed how crime is committed as we move into the 21st century.

I have chosen about five areas of new technology offenses. I started with child pornography because I am struck by the growth of child pornography offenses that has taken place as we have seen the rise of the Internet. And, in some ways, transmission and trafficking in child pornography, while it may seem like a very visceral kind of crime, actually can be seen as a paradigmatic Internet crime.

It takes advantage of many of the Internet's capabilities of reaching millions of people and believing that you can conduct your affairs anonymously without getting caught. You can create communities of interest with people you have never met, just because you share perhaps an interest in this illicit subject matter.

The copies that are transmitted over the Internet because they are transmitted digitally can be made as perfect copies. And this can be done instantaneously and worldwide. So, for all of these reasons, we have seen just an explosion of child pornography cases.

And there has even arisen the problem of what is known as "virtual child pornography" where, with the advances in imaging technology, it is very hard to actually prove in all cases that the image of the child

actually relates to an actual human being. These images could conceivably be generated, and that creates interesting issues of proof.

The second area is intellectual property crimes, copyright infringement. The notoriety that has come with Napster and some of the other large-scale copyright infringement cases; and the great deal of concern of the motion picture industry, the computer industries, the recording industry, all demonstrate how the Internet has profoundly changed the crime of copyright infringement. And there is a new guideline that was just implemented in May to address that.

Another area is computer impairment—such as computer hacking—that causes impairment of integrity or availability of computers. We just heard a very evocative presentation by Richard Power about the scope and scale of that crime.

We also have privacy and confidentiality crimes; there is a great concern among people today that their privacy can be violated with ease. There is also a great concern among corporations that their trade secrets can be stolen with ease. Again, the same properties of the Internet—the ability to transmit perfect copies, instantaneously, to potentially millions of people—create the same kind of concerns in privacy crimes as they do in child pornography crimes and copyright infringement.

As Mr. Vatis mentioned earlier, in the computer hacking cases, there is an added concern because there is so much international computer hacking that it makes it that much harder for law enforcement to investigate.

The final area that I will be discussing today is large-scale consumer fraud. You saw the thousands of complaints that the Internet Fraud Complaint Center has received—even with the limited amount of public outreach they have done—and how much interest there is because the Internet is so prone to consumer fraud, especially these auction websites where people bid, send in good money, and don't get it back.

And, suddenly, the fraud isn't being committed on the corner so that it can be handled by the local police. Suddenly, it is being committed by somebody many miles, many states, maybe many countries away. It can be very hard for someone to get relief. And that fraudster can commit his crime on an unprecedented scale because, with the Internet, he can reach such an enormous market.

So all of these crimes, taken together, give us a broad view of how the advent of cyberspace really is changing things. So now let's take a brief look at how the sentencing guidelines have responded.

First of all, child pornography uses guidelines 2G2.4, 2G2.2. Whether it is possession or trafficking, there is a base of 15 or 17, and the guideline has a special enhancement of adding two points for the use of a computer because the guidelines recognize that the computer can be such a key tool in facilitating the offense. There is also an addition of five for distribution for pecuniary gain. (See Figure Goldstone-1.)

I have worked on a couple of kiddie porn cases in my career at the Department—primarily, we do hacker and intellectual property cases—and I don't know what the definition is of pecuniary gain is in this context. I know, in the software piracy context, we will often use bartering as an example of pecuniary gain—and I don't know if that is also used in this area—but bartering is very common on the Internet as a way of exchanging intellectual property, and I suspect also in the child pornography area, as well. In the

intellectual property area, we would definitely treat that as pecuniary gain. It has even been recognized by Congress in 1997, and I just don't know how it is handled in that area.

Copyright infringement, again, is another example of reaching a wide market, being able to infringe upon software with ease; and, again, this is a software, as the point was made from the audience—Director Freeh has recognized and others have recognized that the creation of intellectual property is, in some part, a key element of our new economy. Software is where the money is, and it is protected, in part, by the copyright laws.

The Sentencing Commission recognized that the old guideline did not fully reflect the loss, did not fully account for it, and on May of this year, after hard, long work, came out with a new guideline. Again, there is an addition of two for the use of a computer. (See Figure Goldstone-2.)

And, in another important change, the old guideline had set the value for calculating loss with the value of the counterfeit item. The new guideline, particularly in most Internet cases, will use the value of the legitimate item. That is an important difference in calculation because, if there is a website that is giving away counterfeit software for free, then the defendant can argue that the value of the infringing item, the counterfeit item, is zero; whereas, the value of the legitimate item can be very great.

And the easy availability of counterfeit software can substantially undermine the market for legitimate software, so it really does cause a great loss to the victim. Even if the person committing the crime isn't personally profiting, that doesn't mean he is not causing loss.

There is a recognition in the guideline that there might be a two-point reduction if there was no commercial motive. And there is a special skill adjustment if de-encryption was involved.

A third area of a new technology crime is hacker crimes, computer impairment, the kind of crimes you heard Richard Power and Mike Vatis talking about. While the guideline basically reflects a 2B1.1 guideline, there is a special instruction of a minimum sentence of six months. (See Figure Goldstone-3.)

The reason that that guideline requires a floor of a 6-month sentence is because, as Mr. Power pointed out so dramatically, it is so difficult in computer hacker cases to value the loss. You are often talking about an intangible loss, a loss of goods. And, while there are some ways of doing it, the guideline does have a recognition that, for computer hacker cases, there should be a minimum sentence of six months.

The one crime area that I am discussing today that doesn't have any meaningful adjustment for computer cases is privacy or confidentiality crimes. In this area, I am going to talk about three crimes; the first is wire-tapping. (See Figure Goldstone-4.)

Wiretapping, when it is committed criminally, has a base offense level of nine, and then there is just an addition of three for commercial gain. I just had a case in Miami of a computer hacker who had installed a sniffer on the computer systems of the Department of Defense, the Defense Threat Reduction Agency, and he intercepted over 3,300 e-mail messages that were confidential to the Department of Defense, as well as intercepting over 20 user names and passwords.

He was a juvenile, and he was sentenced as a juvenile, but if he had been an adult, the guideline would not have reflected any sense of scale for the amount of wire-tapping. Another thing that juvenile did was to hack into NASA computers and download $1.7 million worth of software, proprietary software that NASA has contracted with a large defense contractor to develop. And it was software that controls the environment on the International Space Station.

Now, that is a theft of the confidentiality of NASA information. It wasn't a real-time wire-tap. He just stole the information that was stored on their computers, and that would have been a violation of 18 U.S.C. § 1030(a)(2). If it had been a trade secret that he had stolen, it would have been theft of a trade secret, under the Economic Espionage Act, 1832. Either way, the guideline base would be four because it is a 2B1.1 guideline, and the analysis under §2B1.1 is that the loss is the value of the property taken.

Now in this case, we would value the property taken as $1.7 million because that is how much NASA paid for the software. I don't know if I could persuade a court to use that $1.7 million because the counter argument would be, "Yes, that is how much was downloaded, but what did NASA lose? Did NASA lose anything because he downloaded that software? They still had the software. The software wasn't modified. Is that really the loss?"

And what did the juvenile gain? And it would be very difficult for us to prove what, if anything, the juvenile gained in a tangible sense. So, we didn't have to go to it in that case. There are many other cases where you don't have a clear loss figure; you just have a theft of a trade secret. It can be very difficult to value.

The guideline simply says an upward departure may be warranted if the valuation doesn't fully capture the harm. But, as I say, there is nothing in the guideline that is any more definitive or specifically takes computers into account.

The final area is the one represented by the Internet Fraud Complaint Center, and that is large-scale consumer fraud. Of course, in a usual fraud case, a wire fraud—say 1343—you would just go to §2F1.1, and there is an addition in the guidelines of two for mass-marketing. That mass-marketing increase is useful in computer cases. If somebody is conducting an auction on eBay on a large scale, that mass-marketing exception will kick in. So it is helpful to recognize that fraud on the Internet is different from fraud on the street corner. (See Figure Goldstone-5.)

Now, if the fraud involved computer hacking—again the guidelines have in them for a 1030(a)(4) case a six-month mandatory minimum.

Just to compare and contrast the six kinds of crimes—I gave you the base offense, and then I said, "Let's assume that the offense was committed with a computer and that there was $100,000 worth of loss." But, just assuming that there is $100,000 worth of loss and assuming a typical case, I put together this chart. For what it is worth, the highest guidelines go for child pornography, consumer fraud, and copyright infringement; and the lowest guidelines would go for wiretapping and privacy offenses. Computer hacking would be in the middle, but there is a six-month mandatory minimum. I am presenting this particular chart not to prove any point, but I hope it is food for thought.

A few words on the Computer Crime and Intellectual Property Section—this isn't exactly a paid advertisement, but it is a little bit of an advertisement. We have about 20 attorneys in the Criminal Division,

and we are a general resource to the Department of Justice and to law enforcement, federal and state, on computer crime cases, intellectual property cases, and more generally, cybercrime cases.

In fact, we have a website that Mike Vatis referenced in his remarks, *www.cybercrime.gov*, and we have many manuals there, many Department of Justice reports, and many press releases about these cases. We try to keep that updated, and I have provided the section phone number there. Our section chief, Marty Stansell-Gamm, and deputy chief, David Green, are here, as well. I will be happy to take any questions, in the few minutes I have remaining.

QUESTIONER: My question is about the NASA hacking case where they took $1.7 million worth of software. You said you would have argued that if the person was an adult, he should have been sentenced as if he had stolen $1.7 million and there had been a loss of $1.7 million. Do you think that is appropriate? Do you think that that person, if an adult, even if he just stole it to look at it and said, "Oh, this is not something I am interested in," never used it—should be sentenced as if he had committed almost a two-million-dollar fraud?

MR. GOLDSTONE: You know, I think that is an interesting question, and I think it really does depend on the facts of the case. But, in many cases, I do think that the value of the information is a key figure for the loss. Privacy is an important value, and in some ways, the privacy loss may actually be beyond $1.7 million. Actually, the sense of violation, the sense of jeopardy, the loss is actually perhaps unknown.

One point seven million happens to be the figure that we can fix on in that case. The fact that the person committing the crime didn't have a use for it doesn't mean the loss was substantially less; although, after a long investigation, it did happen to reveal that. There are many investigations where the loss is deeply felt and the investigation isn't fruitful.

QUESTIONER: The E-Signature law that just passed, is that going to increase your business like a million-fold where, now, any person can go on their computer and can give away all their money without a required signature if they just tap a button on their computer and all these companies don't want to wait a day to get something in the mail?

MR. GOLDSTONE: That is a good question. The E-Signature law actually was passed over the summer and just went into effect 12 days ago, as of October 1st, and it generally provides that signatures made electronically shall not be denied purely because they are electronic.

On the other hand, even before the law was passed, we have seen an enormous growth in electronic commerce. People have been able to buy books from Amazon or, on the other hand, be defrauded on the Internet without this law being passed.

So, while it may increase confidence, the kind of consumer concerns that might be foremost are somewhat protected by the law because the law has many exceptions for consumer protection provisions. For example, there were concerns that companies might try to save money on recall notices by sending e-mails rather than sending a letter and that, if people don't check their e-mail, they won't get their recall notice. And those letters are an important means of consumer protection.

There is an exception in the law saying that, while in general, electronic process can satisfy laws that require a written process, that is not true for recall notices and a few other categories of notices. So I think that there are enough protections in the law to generally protect consumers.

But, of course, as there is more growth of commerce on the Internet, there is going to be more growth of fraud on the Internet. And that will increase business probably more for the Fraud Section than for the Computer Crime Section, but we will work hand-in-hand.

QUESTIONER: From your standpoint as a law enforcer, would you rather see the basic approach to these punishments be a loss table with adjustments as the case warrants or start out with a guideline geared to the nature of the activity, with amount itself being the adjustment in appropriate cases?

MR. GOLDSTONE: I would say that, right now, my experience has been that it is very difficult to value the loss in many cases.

You hear companies say, in computer hacker cases, that the way they are going to try to value the loss is they are going to multiply the minutes the computer system was down by the cost of the computer system by the whole year.

That is a very mathematical-sounding way to determine loss. But, of course, we all now that, when the computer system is down, work stops, and how do you value work stopping for an organization? It is very difficult to value.

So, at least in the near term, I find that some skepticism might be in order for these mathematical calculations which may undervalue or overvalue the loss; whereas, the specific adjustments that you referred to are very helpful in determining it.

Now, as time moves on, we might see improved techniques that would enable us to use tables better. Is that a fair answer?

QUESTIONER: It almost sounds like you prefer the latter; for example, you could just have a guideline for intrusion into a system, and then adjust for value if value is calculable. But you start with a crime of intrusion into a system.

MR. GOLDSTONE: Yes.

QUESTIONER: Would that be your preference?

MR. GOLDSTONE: I think that, at least for now, that can be helpful because, in so many cases, it is so difficult to value the loss.