KEYNOTE ADDRESS

PROSECUTION RESPONSES TO INTERNET VICTIMIZATION

The Honorable M. Jane Brady∗

JUDGE BRADY: Well, thank you very much and welcome to everybody from all over the country. I wanted to say thanks to Tom Clancy and to Ole Miss for this invitation and for the existence of the National Center for Justice and the Rule of Law. It is just a tremendous program.

I first came down here at the invitation of then-Chair of the Criminal Law Committee for the National Association of Attorneys General, Patrick Lynch of Rhode Island, who had a conference here on Internet crimes. And, when I went home, it was kind of neat being able to tell people I had dinner with Tom Clancy. Everyone assumed that I knew the author of The Hunt for Red October and had the inside story on that. So you have a nationally recognized name, and, I believe, a nationally recognized program.

The outstanding aspect of this program is that it honors

∗ Superior Court Judge, State of Delaware; Former Attorney General, State of Delaware
the prosecution function and puts it on an even balance, unlike many of the law schools around the country. It recognizes the valuable public service asset that prosecution is. In many law schools around the country their public service programs are to help the indigent or to help people with the civil litigation issues of victimization in domestic violence, but they fail to include, even if they have a prosecution externship program, they fail to include it in their public service array. I think it is really forward thinking to have recognized the value of the public service of prosecution.

As I said, I was here in May of 2005 and we went through an entire conference on Internet crime and I went up to Tom and said, "Do you realize that, in this entire program, I think we heard the word victim twice? There's a whole aspect to Internet crime that goes beyond the hardware and software and detection devices—the people who are at the other end of that Ethernet or phone line or wire." And, as a result, this conference was initiated.

I was very honored when they invited me to come back as the keynote speaker for this conference. Let me explain that the reason I served on the National District Attorneys' Association Board of Directors is because, in Delaware, the Attorney General is the DA. Rhode Island and Alaska are the other two states where that is true. And so, we have no elected prosecution officials on a countywide basis. I had the enviable opportunity to serve, not only as the attorney general, but also as the district attorney for my entire state and we prosecuted, literally, tens of thousands of crimes a year. And, I was a prosecutor in that office for twelve and a half years before my election.

So, I have personal experience with the victims of crime in handling my own cases as well as the perspective of policy, broad legal parameters, and the social issues as a result of my experience as attorney general.

About four months ago, as Tom said, I was appointed to the bench. My tasks and responsibilities have changed. But I don't think that, so long as I keep my remarks balanced and factual, that I will give reason to the concern that my superi-
ors on the bench had regarding speaking about victimization at this conference.

So, now that I have given that disclaimer, let's get on to what I really want to talk about, which is how do we deal with the issue of victimization in these crimes? And, what are the special issues related to victims of Internet crime? I have put together an outline and some comments as to a number of issues, but let me say, first and foremost, that you are going to get a lot of statistics.

I've looked at the tremendous materials in the booklet that you received and have noted the tremendous qualifications of the speakers who are going to come after me. I want to try to give a broad overview of why this issue is important to victims and should be important to you, in terms of assisting victims, but I also put together this outline that takes us from the detection and the investigation to the prosecution and the resolution, because, of course, we all know that the prosecution is not the end of the case for victims. We also need to consider how to help resolve their victimization. And I am going to follow that outline generally, but I will also be extemporaneous on a few occasions based on some recent events and your comments.

I also wanted to comment on the array of services that Attorneys General's offices offer because Jonathan Raven, from the California Attorney General's office, and I worked on a survey last year of Attorneys General offices around the country, which showed that about seventy-three percent, if I recall the number, offer a victim service component. So if you, in your capacity, don't have regular contact with that component, then I encourage you to do so. Get to know where in your office that sits, who in your office provides the services, whether they are well utilized, whether they can be better utilized. Most instances of the crimes that you are going to address at this conference are going to fall to your offices, even in jurisdictions with active District Attorneys, more than most other types of crimes. That is because there is considerable expense, equipment and expertise that are required to investigate and detect these crimes. There have already been
regional and federal initiatives on training, and there are going to be more, and the larger offices, with more training dollars are going to be looked to for assistance.

Today the real world is the cyber world. When you look at a survey that was done by PUE, the Internet project, they found that seventy-two percent of all adults use the Internet and eighty-four percent of people eighteen to twenty-four. Eighty-four percent! Eighty-three percent of people thirty to forty-nine, so, overwhelmingly, anyone under fifty is on the Internet and the statistics show that. Interestingly, seventy-nine percent, which is a higher percentage than most of the other breakdowns, of English-speaking Hispanics are using the Internet.

This was a national survey conducted between September of 2004 and May of 2005. Nearly ninety percent of those people who have a college degree and make more than forty thousand dollars use the Internet and the majority of them identify home Internet use at nearly the same rate as they identify office Internet use. Involvement with the Internet is not just associated with the workplace; it is also in the home. And, when asked, “Why do you use the Internet?,” only about half of them said they use the Internet to do research for work; ninety-one percent of them use it for email. By the way, in my research for this conference, I also learned that the average American worker that has a computer at work gets about ninety emails a day. Talk about Internet victimization!

In addition, of course, many of them use the Internet for research related to their personal interests, directions, and other similar purposes. Interestingly, by the way, in the same survey, conducting banking or purchasing stocks, things like that—about twelve, thirteen percent. You hear a lot about adult content on the Internet and dating services on the Internet and the associated victimization issues that they hold. In the survey, only four percent admitted to viewing anything with adult content on the Internet and only nine percent admitted to looking for Mr. or Ms. Right on the Internet. That is a very small percentage, actually, compared to what the perception is about such use. But, as you can see,
the reality is that today the real world is part of the cyber
world. And it is going to impact people in very, very real ways.

Now, much media coverage, and therefore the prevailing
perceptions, of Internet victimization is largely regarding child
solicitation for sex, financial scams and frauds, pornography,
or hacking. And, I will address those, but first, I want to talk
about the broader picture.

Let’s first address detection. The detection of Internet
victimization can prove very challenging. If you were to Google
“Internet victimization,” which I did just to see what would
come up; you would get one million, one hundred ten thousand
hits in eleven hundredths of a second. So if you are a police
officer trying to sort through what’s going on on the Internet,
you are going to be inundated and you’re going to have to be
very specific and try and detect the kinds of crimes that are
occurring on the Internet through more discerning investiga-
tive tools.

There is clearly public awareness of the fact, as evidenced
by all of these articles on Internet victimization, that it is oc-
curring, but detection remains very elusive. Legal issues about
where the victimization occurs when it is Internet crime. Prac-
tically, it occurs inside your bank account, inside your IT sys-
tem, inside your living room, and, in many instances, in the
context of serious and violent crimes, although they involve
remote contact, it invades right into the victims’ mind. It af-
flicts the victims’ sense of well being, security, and safety.

The impact is particularly challenging for victims if, like
in so many instances, they are participants in the crime be-
cause they either responded to an email, or invited contact, or
somehow engaged with the perpetrator online. There are a lot
of additional issues that these victims have to address, many
of which we most often have seen in domestic violence or sexu-
al abuse cases, but now can occur in many other types of cas-
es. And, instead of personal confrontation, the way that these
offenders get into your living room, or into your business, or
into your bank account is not with a gun, it’s remote. They
don’t put themselves at personal risk to commit the crime.

And so, the usual methods that law enforcement has used
to detect crime—fingerprints, hair and fiber transfers or DNA—are really not available to help the police. And that kind of evidence is not only useful in determining the identity of the perpetrator, but can also provide other clues, such as the manner in which the crime occurred, and the location or locations where the crime occurred. Those questions are not so easily answered when the crime is committed through the Internet.

The fingerprint could be oceans away and the identity could be a pseudonym, the true identity of which could be very, very difficult to find. I mentioned earlier that one of the challenges is determining where the crime occurred. Now we all know there are the occasional issues of jurisdiction and territorial disputes. You know the usual territorial disputes—"It's mine. No, it's mine. No, it's mine." And everybody wants to prosecute the crime. Well, with Internet victimization, it could easily be, "It's yours. No, it's yours. No, it's yours." This occurs because the laws may be unclear or because the expertise and expense in both detecting and following through with the investigation and successful resolution of those criminal cases is so difficult.

There are challenges to educating and equipping law enforcement to be able to detect and investigate these crimes. Some efforts have been undertaken. There's a new training center in San Diego, which is a pilot for a number that are hoped to be located around the country. This kind of training for people who are assigned to detect, investigate, or prosecute Internet crime is critical. These professionals need to have an understanding of the hardware and software issues, to understand the mechanics of the technology.

Getting the cooperation of business is very important in the successful detection of Internet crimes because the Internet service providers are the people that are the key to finding out who lies behind—what face lies behind some of those crimes. I recall my frustration with the unsolicited spam emails, particularly the pornographic ones. I found out that every time you click on the link and go to the site, there's a penny or two pennies that is paid to the person or entity
which sent it.

So I told my investigators, "Let's follow the money." Well, it was not as easy as I thought it was going to be. And getting cooperation of the Internet service providers is important. Virginia was able to do that with AOL a few years ago in an incredibly successful prosecution, one of the first in the country. Delaware has a great law on the books. We haven't really been able to use it very much because we don't have the information to be able to identify the perpetrators and bring them to justice.

Now let's take a look at detection from the victim's perspective. I saw in the materials that you are going to talk a little more in depth about this, but many Internet crimes are not reported, particularly financial crimes. As any of you who have worked with seniors who are scammed over the phone, who are scammed at their front door, or in an affinity fraud scheme know there is a great deal of embarrassment and a great deal of self criticism about their exercise of judgment. They are reluctant to report it; they are reluctant to acknowledge that they were a victim of a fraud.

There are reasons for that. If you are twenty-nine and make a stupid decision and are victimized, you and others conclude it is because you made a stupid decision. But, if you're seventy-nine and you make a stupid decision and are victimized, everyone thinks you are beginning to lose it. And so, there's an incentive for older people who don't want to lose their independence not to report these crimes. Similarly, with financial crimes over the Internet. In the same study to which I previously referred, about thirty percent of people over sixty-five are using the Internet on a regular basis. My dad is eighty-one, and he is a day trader. He's got eight monitors lined up on two shelves over his computer. And so, he's very active on the Internet. But others, like my mother, use the Internet mainly for email. But, even though there are only about thirty percent of those over sixty-five on the Internet, they still are targeted. Specific scams are intended to appeal to individuals who are retired, on fixed income, or a veteran. Many of the scams are intended to reach out to people who
would be more likely to respond because of their life experiences, and their status or situation in life at sixty-five or older.

But, it’s not just the financial crimes against individuals that go unreported. Law enforcement faces the same situation with financial crimes against businesses. You are going to hear some more about this, but it’s true. Businesses and even the government are afraid to report a hacking because the fact that their system could be compromised because it could encourage someone else to do it. And, there are other scams against businesses. False invoices is a favorite one. A false invoice will be sent over the Internet, complete with authentic-looking letterhead or logo, for services that have been rendered. The bookkeeper pays the charge, and, in many instances, that is the end of it. If they are careful and not too greedy, these scam artists can get away with a lot of money. Even when detected and even if it involves a substantial amount of money, businesses are very reluctant to prosecute. They are willing to suffer their losses, and they don’t want to be involved with the court system or with the police in the investigation or prosecution of the case.

They also, though, don’t want anybody to learn, either from testimony in a trial or otherwise, how a person hacked into their system or where the gaps are in their security. There’s a group called InfraGuard that has worked with businesses to try to prevent technology crimes, so that victimization doesn’t occur.

InfraGuard is a federal program under the FBI that works with businesses to not only prevent, but also address hacking and other kinds of economic terrorism that might occur. I went online the other day and paid a bill in four seconds. It was great. We can do so much on the Internet, but we are so vulnerable with regard to access to all our personal information. And while we are not addressing international issues in this conference, you should know there are actually websites out there, most of them outside this country, that sell your personal information and your accounts online. Suppose they have access to an account in a credit union with forty
thousand dollars in deposit. They will sell it on the Internet for five hundred dollars. And they actually post that product online. So, there's a lot to be said for assuring that your financial institution has the best security possible. The InfraGuard program's public-private partnership is working very, very hard to assure good integrity in the technology that supports the financial, and other, institutions in this country.

But, while uncertainty of one's own judgment may be an issue in Internet financial crimes, in the other kinds of crimes that we have talked about and you are going to see in your materials on Internet victimization—the child sexual abuse, the pornography, the solicitation for sex—there is a new element that those who assist victims must acknowledge. Many of them, fortunately, when they are reported, are detected in time to avoid significant harm. If the child reports something or the parents suspect something is wrong and the crime is detected in time, the police pretend to be the child and they intercept the offender before he has access to the child that he solicited online. The crime most feared has not occurred, but the imagination of what might have happened could exceed even the crime that might have occurred. And, for those instances of bullying and the other kinds of harassment and intimidation that occur on the Internet, there can be significant psychological reactions that present real challenges for you to deal with in serving those victims.

First, the young victims, let's talk about those because there are some findings I think are very concerning about those crimes. At least, according to a survey that was done by one child-oriented organization, about fifty percent of the kinds of threats or incidents that should have bothered children, the kids said didn't bother them. So I started thinking about that result and about what was going on with kid victimization and it occurred to me that maybe kids don't really see the cyber world as a real world. Maybe they see it as a fantasy world.

An incident in Delaware recently helped substantiate that thought. A local radio station disc jockey went onto a website similar to MySpace.com where kids from the local high school
were posting pictures and descriptions of themselves. In one, a student had a gun, and he and a number of the other boys described themselves as “gangstas.” Girls were describing themselves as “hos” and they were showing pictures of their buttocks and doing things that they did not normally do. They became very upset when the radio announcer read from the website, without, mercifully, using their actual names. They were incensed that he had invaded their privacy. It was a very enlightening moment for me, because they had no appreciation of the response they were inviting by what they were doing.

I saw how vigorously these kids reacted and were offended. They called into the radio show, they picketed, they were very offended that someone would take their personal information and put it out on the radio. They failed to appreciate that it was on the Internet for everyone to see. Many of them engaged in this banter that could get them in over their heads, not appreciating that it is real.

I am very concerned that they will not appreciate what can occur unless we educate and inform these young people. There are girls and boys, today, who are putting pictures of their buttocks, breasts, and genitals on the Internet. They fail to appreciate that first, it is publicly displayed; and second, that once one person downloads it, it is there, potentially, forever. It is there, potentially, forever. So it is important that we inform kids about the fact that these exchanges are not just between them and that is not just their space, that it is cyberspace. And that Myspace.com is in every space.

We have all heard the stories about the undercover police officer going online, posing as an eleven year old girl, or pretending they are fifteen and buying Viagra online. The truth is that the police can detect and investigate these crimes as remotely as the offenders. Instead of walking the beat, cyber detectives are letting their fingers do the walking. And they are getting pretty good at discerning how they should work to detect the kinds of predators that work online.

I meant to bring a statistic with me and forgot it. Maybe one of the other speakers will cite it. Several studies have
found that approximately one in five kids reported having received a sexual solicitation online. The most remarkable thing, and the statistic I can't put my finger on, is that in the chat rooms, when the predator thought that they had a victim or a potential victim, the conversation turned to sex within thirty seconds or sixty seconds of the contact. The study found that after three or four IM exchanges or chat exchanges, they were already approaching sex. Know why? They don't want to waste their time. They don't want to waste their time. And so, for kids who are unprepared for any such event, a situation can get out of hand very quickly.

Now, suppose the police have done a great job of detecting and investigating a crime and they figured out who did what and they bring it to the prosecutor, or your office. You look at your laws and you think, “Okay, I'm supposed to prosecute this case. What law was broken?” Harassment, stalking, the way that we traditionally have defined those crimes, does not include anything except personal contact. Delaware and most states did add contact by phone and mail. But, over the past several years, states have had to again change their statutes to include crimes committed by computer and Internet because they were not included in the previous statutes. And so, did it fit? Did it not fit? We argued the phone line back in the old time days of dial-up access to the Internet, which only thirty to forty percent now still use.

We argued that access was by the phone line and that the instrument at the end of the line didn't matter. We never went to trial or had the court resolve that issue, but that was one of the ways we tried to approach it. How many of your states, now, have added a specific Internet or computer crimes that would apply to harassment and stalking and everything? I see a little over fifty percent, have responded affirmatively.

When you go back to your offices, look at your laws. You know the attorney general is a statewide official and can be very effective in getting the state statutes changed to adapt to the changing technology by which criminals are taking advantage of the legislature's constituents. So go back and look at your laws. And if your laws are not adequate to the crimes
that you are seeing and you are going to learn a lot more about in detail through this conference, look at your laws and make proposals to fix them. Look at what the other states do and figure out what will work best in your state. That is one of the first inquiries that you need to make.

So, first line of analysis—"What does the law allow?" If you get an Internet case, what does the law provide? The second is "Where did the crime occur?" Many times, the issue of the location of the crime will be resolved in the prefatory sections of your criminal code in your state. The code may say that if any element of the crime occurs in your jurisdiction, you can prosecute. Others say, if the overt act by the perpetrator occurs in your jurisdiction, you may act. And there are some which provide that if the harm to the victim occurs in your jurisdiction, you have authority.

So, figuring out whether you have jurisdiction to prosecute this crime is another issue. To the victim, that means a great deal. If you don't have authority to prosecute the crime where the victim is, it is another impediment to getting their cooperation and successfully prosecuting a person who's committing a crime because that victim will be required to go to another jurisdiction.

And, if you are talking about young victims whose parents are concerned about them participating in a trial where the offender will be able to see the victim—remember, the offender likely never knew what the victim looked like before. It is going to be a significant impediment to keeping their cooperation if they have to travel to another jurisdiction and may never develop a rapport with the prosecutor or victim services worker.

So, consider what is, for the victim, the best place to be for prosecution. Look at your laws and figure out where you can prosecute the crime. And, while not all your victims are necessarily sympathetic, they all are vulnerable. So, how do you provide victim services to these victims?

I am not going to talk about how you generally provide victim services to victims of certain kinds of sexual crimes or domestic violence crimes or stalking crimes because you've
done that. But I will talk about what happens with the victims in certain situations—I call them the balks. Everybody knows baseball? Okay. The balk is where you start the pitch and you don’t let go of the ball. Okay? And it’s a penalty.

That can happen to victims in these Internet victimization cases, particularly the solicitation cases. In those which are detected or reported, the greatest harm that could have occurred does not. The fear of what might have happened is, however, often more difficult to face than the certainties which other victims to whom a harm has occurred learn to address. The latter have some tangible event, some consequence, which they can address emotionally, try to understand, and with which they can begin to cope. Often, with Internet victimization, the actual event is a balk, and the fear of what might have happened can be very, very devastating to family members and to the victims themselves. It can become their very own version of terrorism that prevents them from appropriately interacting and engaging socially and at work.

And so, there may be unique issues in serving these young victims and their families who sit and worry about everything that might happen now because they can’t associate one bad act with one bad person. Just as the Internet is ethereal, there is an ethereal threat that is ever present to them.

I mentioned, also, that many of these victims lose confidence in their own judgment. This applies not just to financial fraud victims, seniors and others who are challenged.

Finally, for victims, it is not just the success of law enforcement or the prosecutor. For victims, it is “How do I go forward—emotionally and psychologically?” There are some things that are being done for victims of Internet victimization. The National Organization of Victim Assistance is a group with which I served, which has often dealt with crisis response. Their models of crisis response for these balk cases I was talking about, many of the responses for crisis—models for crisis response—can work for this kind of Internet victimization, where the fear and the anxiety and the emotional response is one that is of a lingering and continuing nature.
And, finally, how do you help the families of these kids with resolution? Just as in some rape cases, in which the family, who has been a protector, feels that they have failed, the same can be said in these Internet crimes. The guilt may be even more significant, however, because often in these cases the parents provided the computer or didn’t monitor the child’s use of the computer. They may have allowed the child to have a computer in the child’s bedroom. In the realm of providing victim services, you need to consider those secondary, as we call them in Delaware, secondary victims, that is, those victims who are related to and affected by the victimization of the direct victim of the crime.

I’ve looked at the materials for this conference; they look tremendous, as I said. You’ve got some excellent speakers. This conference is going to provide the very best overview that I have ever seen on this issue, and good information on all aspects of Internet victimization. I hope that my overview has covered both the importance of being aware of and educated about Internet victimization and the role that you can play in the attorney general’s office by reviewing your laws, educating your law enforcement, looking for where the financial resources are or the expertise is to draw upon to assist local jurisdictions in the prosecution of Internet crimes, and to provide adequate victim services for those victims of Internet victimization because, as I said, there are unique issues that they face, unique challenges that they pose for you.

And since the majority of AGs offices do provide victim services, this awareness needs to be a component of how you provide those services. If, today, seventy-three percent of all adults use the Internet and eighty-five percent of those eighteen to twenty-four are using the Internet, I think it is a good bet that, of those aged seven to eighteen, probably ninety-five percent are using the Internet. And soon, it is going to be universal, much like the telephone.

So there are some new and recent developments in the evaluation of the extent to which the Internet and crimes over the Internet are occurring and identity theft is occurring, much of which occurs over the Internet. I found a very inter-
esting article about this man in Russia who is selling accounts online. He actually is advertising the accounts online. So, the more remote and the more junctures through which the email is routed, the more difficult it is to find out who’s actually committing the crime.

And, of course, unfortunately, the further you get from home, the more difficult for you to prosecute it no matter what the harm to the victim. And the more international you get, unless it’s a big case, you don’t get the federal government’s interest because they can’t, and don’t, prosecute every little crime.

So, good luck, enjoy the conference. I have to tell you, I spent eleven years as Attorney General of Delaware and I always wondered why anyone would want any other job. Everybody who has held or holds the position says it’s the best job in the world. I, however, had always wanted to be a judge since before I became a lawyer, so I don’t regret the decision.

But you have a tremendous opportunity to make a difference in your state, in the law, in the policy and the priorities of the agencies you represent, to impact the direction of the law enforcement community and the legislature in your states. And so, I encourage you to fully utilize the resources you have at your disposal and address the needs of the law—reforms in the law and in your offices to respond to crimes against your citizens via the Internet. Thank you very much for having me.