THE DECISION TO PROSECUTE

INTRODUCTION

On April 5, 2006, as part of the Prosecutorial Responses to Internet Victimization Conference hosted by the National Center for Justice and the Rule of Law and the National Association of Attorneys General, two panels were held to focus on pressing issues faced by prosecutors involved in Internet Victimization cases.

These articles are distillations of the two panels. The articles highlight especially relevant portions of each panel discussion and incorporate the speakers’ actual words. For a number of practical reasons related to transforming a panel into an article, the panelists’ remarks have been edited and, in some cases, changed or re-ordered for continuity and clarity. To convey the feel of the live panel, substantial block-quotes have been included which add to the realistic and practical tone of the panels. The panelists appeared on their own behalf to share their experience and insight. As such, their comments were solely their own and not on behalf of any agency or organization.

Both panels were moderated by the editor and consisted
of experts who answered questions prepared prior to the conference before a spirited and insightful audience.

Marc M. Harrold

PANELISTS:

- Terry Berg, First Assistant United States Attorney, Eastern District of Michigan; former Chief, High Tech Crime Unit, Department of the Attorney General of Michigan
- Patrick Corbett, Professor of Law, Thomas M. Cooley Law School; former Deputy Chief, High Tech Crimes Unit, Department of the Attorney General of Michigan
- Todd Lawson, Assistant Attorney General, Office of the Attorney General of Arizona
- Thomas Sadaka, Of Counsel, Berger Singerman; former Assistant Statewide Prosecutor, Office of the Attorney General of Florida

"There's no way that any office can prosecute every case."

This statement was the starting point for a panel discussing the factors that contribute to a prosecutor's decision whether or not to prosecute a particular case involving Internet victimization. The Panel's goal was to provide information in an attempt to answer, or at least come to better terms with, the following questions:

QUESTIONS FOR PANEL:

1. What is the role of resources in the decision whether to prosecute?
2. What is the role of multiple jurisdictions (victims, perpe-

---

1 Senior Counsel, National Center for Justice and the Rule of Law; Visiting Professor of Law, University of Mississippi School of Law.
2 It should be made clear, at the outset, that the statements and opinions offered by the panelists and moderator are solely their own and are not offered on behalf of any organization or agency.
trators, witnesses, etc. and the varying levels of prosecuting agencies (i.e., federal, state, local) to the decision whether to prosecute?

3. What role do the characteristics of Internet victims or their experiences play in the decision whether to prosecute?

4. What are the policies and procedures related to case acceptance or denial?

5. What are the challenges in dealing with law enforcement in Internet victimization cases?

QUESTION 1:
What is the role of resources in the decision whether to prosecute?

An underlying theme of the panel was that there are several major, limited resources that influence the decision to prosecute. The following discussion focused primarily on money, time, staff and technology.

PROFESSOR CORBETT stated from the outset that “budget is a massive concern in this area, whether it is setting up the [cyber-crime] unit, buying the equipment, and then having witnesses and victims that are all over the country.” Internet victimization cases generally take a great deal of time. In some cases, administrators (i.e., “bosses”) do not have the same level of interest, experience, or understanding of computer cases [as their subordinate prosecutors]. This can lead to under-prioritization or supervisor criticism that a prosecutor is spending too much time without yielding results. PATRICK CORBETT conveyed his experiences in Michigan:

What I have seen in Michigan—and possibly this is occurring in your states—is unless you have prioritized this as an area for prosecution and have higher ups/bosses who understand the time it takes to be able to investigate and prosecute these cases and that you might do a lot of investigation for a lengthy peri-
od of time, expend a lot of resources, and might not get anybody at all. You might find out that they're in Russia and you can't get them. Unless you have that mentality from the top down, it's difficult to do any cases other than sexual predator [cases].

It also came to light that it is not only the resource limitations of the attorney general's office, but also the resource limitations of the investigative agencies which may, or may not, be part of an attorney general's office that can influence the decision to prosecute. For example, in Florida, all of the investigators in that constituent office are civil investigators, leaving prosecutors somewhat at the mercy of decisions made by the administration of outside law enforcement agencies. In some cases, TOM SADAKA reported, the result was that no investigation took place at all: "Generally, [outside law enforcement agencies'] budget concerns are more of an issue because you can't even get them to invest the resources necessary to investigate the [computer crime] cases, because they're just too costly."

To illustrate this separation between prosecutors and law enforcement in the Internet victimization area, TOM SADAKA stated:

A couple years ago I modified our identity theft statute to include a paragraph that said that the case could be investigated or prosecuted where the victim resided or where any element of the crime occurred. [This was] simply to make it easier for local law enforcement when their citizen victim called in and said, "Hey, I've been the victim of identity theft that happened in Utah."

The local office no longer had to say, "Well, that's outside of our jurisdiction." The response I got, and this speaks directly to the budget, was hate mail from the sheriffs, and phone calls saying, "All right, so you're going to give us the money to go investigate these cases, too, now that you've made us do it?" I
said, “Well, I really haven’t made you do it. I’ve just created an avenue so that you can.” But that’s all purely a budgetary issue.

The following is a paraphrase of the ensuing conversation among the Panelists and audience:

If you have fifty complaints, but twenty of them are on one guy, they’ll package up those twenty consumer complaints for eBay fraud or for identity theft or however they’re coming in. They’ll package up twenty people and they’ll send over to me and say, “Hey maybe this is a guy you can investigate.” [This] helps keep us focused on the most-efficient cases. This is especially true from the detective’s perspective.

If you are a street detective and you’re working an Internet crime beat or an identify theft beat, you almost have to work every little angle, because all the cases in this area start with one complaint on a small amount, $50.00 loss or a $500.00 loss. It’s when you kind of get to the source of it and you look at the bad guy’s computer and, whoa, he’s ripped off 2,000 people at $50.00 a head or $500.00 a head—that’s when you’ve bumped into the big case. It all happened because of one little victim. So you have to do a certain level of low-level service to victims to find the big cases that are going to be worth your budget draw.

The panel generally agreed that the decision to prosecute might come down to a type of pragmatic, objective determination. In many cases, that decision to prosecute will hinge on the ratio of a particular defendant’s damage and the aggregate nature of the victimization, whether or not it is monetary. In making that decision to prosecute, distinct from the number of victims and where they are, a number of state statutes have thresholds. For example, if you want to charge an aggravated identity theft, you need to have five victims. So we’ll start to
look for cases that have that accumulation so that you can get up to more-serious charges. If we have one really loud victim who lost $50.00 versus eight or ten victims who each lost $50.00, you start to look for the collectives and the groups and the ways you can get more bang for your buck with the prosecution. Limited technological resources are also relevant and affect the type and number of cases that prosecutors' accept. Most prosecutors' offices are limited to the forensic area:

I can find a detective somewhere to go knock on the bad guy's door. What I can't do is get anybody to search his computers between now and 2009. They're going to sit in a warehouse somewhere until the forensic guy gets around to it. So when we start looking at the victim complaints that come in, we try to do some aggregation.  

In certain instances, the legislature, eager to appeal to the timely concerns of its constituents, passes criminal statutes that will not realistically be enforced. When this occurs, it stretches existing limited resources even farther.

For example, PROFESSOR CORBETT made the following observation about Michigan laws:

Something that has happened in Michigan, and I'm guessing this [has] happened in your states, is [that] the legislature sees a need to pass these new laws. Maybe it's because they just want to have something that says "children" in it and protecting children helps [them] to get re-elected. Especially in Michigan, [as] their terms are limited and maybe this is happening in your states [as well]. So they feel like they have to do something quick[ly], but you [end up with] all these laws.

The clearest example of the budget being a con-

---

3 This is a paraphrased version of conversation among Panelists and Moderator.
cern is with statutes for crimes that no law enforcement officer is even remotely going to consider pursuing.

Michigan recently passed the Children’s Protection Registry Act. I routinely go talk to law enforcement officers about state laws and update them on the laws, and they’re like, “What? This is a criminal statute that exists? I don’t know anything about it. I’ve never even heard of it.” Then I ask “would you ever be able to prosecute a case under it?” [They respond], “Are you kidding me? I have no time for anything but the certain kind of cases that [my] boss[es] have made a priority.” So that’s the clearest indication that budget’s a massive concern to me.

TODD LAWSON provided a final example of how limited resources, especially in victim/witness travel-in cases with a sizeable number of victims spread out geographically.

We had an auction fraud case with 228 victims of baseball card and memorabilia related fraud. When it came time to charging I used a group count—a scheme count and I indexed all 228 as victims. Then, we sent them all notices.

When it came time for trial, we whittled that list down to reflect a simpler pattern so we could make sure we still had enough incidents to prove a scheme. We had enough victims to show a pattern, and to make sure we had a loss threshold. Even if all 228 are not named in the indictment, it is important that they are all counted for purposes of a plea.

If it comes to trial, I ask some of the people up front: “Are you willing to travel?” Usually, I get back the standard, “No, I’m not willing to travel.” In that case I say, “Well I can’t guarantee that you’ll get restitution if we go to trial.” This way the ball is back in

---

*See generally Mich. Comp. Laws § 752.1061 (2004).*
their court.

If we do get a plea, I can put them on the restitution. Of course, the defendant owes no telling how many people so it might be $50.00 a month for the next seven years while they're on probation. So, that may be a loser anyway.

I do believe that in a case where I have the defendant here, [in my jurisdiction] and I have a multitude of out-of-state victims, I'll put them on a count and try to get them victim rights. But, when it comes to trial, I will easily whittle it down to what I need to make a trial manageable. I won't call all 228 [victims].

We had a defendant who was doing large-scale identity theft, and all his victims had been customers of a medical center in northeast Louisiana. He'd obviously stolen some records, or had gotten some stolen records from [the medical center]. First, we had him in Phoenix. So, we prosecuted him there. All our victims were from Louisiana. I could also see the flipside. What if I was in Louisiana and I had a defendant somewhere else and I could make the case in Louisiana where he had stolen all the information? In that case I could bring that case where the victims are if I had a pattern like that.

I don't necessarily think that I need to have the defendant in my jurisdiction. Wherever the defendant is, his computer is. Wherever his computer is, there's a lot of evidence. It's hard for me to call up another state's law enforcement agency and say, "Will you do this for me?" The [U.S.] Postal [Service] guys pick up the phone and they're talking to guys they went through training class with. Being in the task force with the Postal guys makes all the difference. They task people.

I've forgotten how many times I've got a case that's heavily involved in the Fort Lauderdale area. We've found a number of the Postal guys out there basically doing work for the attorney general's office in
Arizona, as a favor to the Postal Inspector in Phoenix. They've done countless hours of work for us. So, that's another advantage to task forces.

QUESTION 2:
What is the role of multiple jurisdictions (victims, perpetrators, witnesses, etc.) and the varying levels of prosecuting agencies (federal, state, local) to the decision whether to prosecute?

TODD LAWSON provided an initial synopsis:

Every case starts off with one loud complainer who's got a $50.00 loss or a $500.00 loss, usually. You have to do a certain amount of due diligence in the beginning to see if it's going to break out into an organization, or if it's going to break out into a guy passing bad checks on the corner. If they have multiple outlets for a task force, the task force will be more efficient.

Because if it's that one guy who is the homeless guy living on the corner who is passing bad checks, police will refer that to a county agency for a bad check. Taking that as an ID-theft investigation might lead to some of the types of cases we've had. We've found prison gangs running ID-theft operations and employees of county government running ID-theft operations.

The more expansive kinds of cases gravitate towards the U.S. Attorney's offices side. So we kind of have the county attorney taking the little stuff and the U.S. Attorney taking the big stuff, and then we [the attorney general's office] get everything else. It works out fairly well in terms of good cases with moderate-sized losses, and usually anything that has an interstate or multi-state angle goes to the U.S. Attorney, so it makes things easier to prosecute. We have the big statewide crime, which is what we're aiming for.

The panel line-up was particularly valuable because there
was an opportunity for state assistant attorneys general to discuss the role of the federal government in accepting or denying certain cases.

In response to a specific question about the role of U.S. Attorney's Offices, TERRY BERG stated:

Well, here's the deal. As I'm sure all you know, I've been in the state system too. So, I've been on the outside looking in. The feds just don't handle as many cases as the states do. Let's face it—the states and counties do a ton more cases than the feds.

So, the bulk of criminal prosecution in our nation is done by the locals and the states. There's no question about that. The other thing is that, and again, when I was thinking about this question of the role of the victim and the decision whether to prosecute, well the decision to prosecute is a broad concept.

It means whether you even want to do the case or not, should we do the case or shouldn't we? It also, I think, encompasses the question of, "Well, what do I charge?" You think you're going to do the case, but now the questions emerge related to the decision to charge and, specifically, what charges to use?

I see the role of the victim probably being more important in the latter area of the charging decision. How to actually craft the charges once you think you're going to bring the case. Because whether or not to prosecute is really, to me, based more on the strength of the evidence in the case, and then whether you have prosecution thresholds of some kind that determine whether or not you're allowed to take the case.

This is sort-of my long way of getting into the federal system. We do have prosecution thresholds, which are usually in financial terms. In the fraud area, they relate to how much money was lost. Our prosecution thresholds are under review right now. By
way of example, let's say that the prosecution threshold for a fraud case was $100,000.00 or $250,000.00. Well then that means that the average identity theft case where someone's credit card was used or their identity stolen and a credit account was opened or some other kind of Internet account was opened, [and] financial damages were incurred, is not going to meet the threshold for a federal case.

So the bottom line is that if we wanted to try and look at it and say, "What kinds of cases would the U.S. Attorney's Office be more interested in or able to take?" The general rule of thumb is really big cases. They would be cases involving a lot of money, cases involving interstate commerce—all Internet cases are this way—but some serious interstate activity occurring in more than one state.

In some instances, these are going to tend to be the cases that most prosecutorial entities would rather keep themselves. Why, because they're really good cases. Due to limited resources, what the federal system tries to do is to narrow down its focus and take those cases that are the most significant.

That's one side of things. The other side though is that through the use of task forces, there can be a very effective sort of multiplier effect in terms of the investigations that can be done. That is a way to leverage federal resources.

Because many federal agencies will want to send a person to work on a state and local task force in the area of Internet crimes against children, those task forces often involve federal agencies. In our district, we have a very effective identity fraud task force that includes state and local officers.

The task force also involves the corporate security representatives of some of the big retailers, like Target®, for example. They've just been great. The task force agents have done a lot of great cases. They're very reactive. They work with certain prosecutors
within the U.S. Attorney's Office, so they get warrants and do complaints right away. They almost work like a drug squad. They'll go out. They'll get information regarding a particular house where ID's are being made or checks are being made, and they'll hit the house. They'll develop information.

They try to go after organizations basically, identity fraud organizations, which are also another sort of buzzword in terms of getting the feds involved. If you have a case involving an organization, a conspiracy, a group, then that's the kind of case that the feds are going to be wanting to focus on more than the individual cases.

So that, I guess, is the bright side of things. Getting the U.S. Attorney's Office to take any particular case may be difficult unless the loss amount meets their thresholds, or the type of case that it is, is significant enough. Through [the use of] task forces, you can leverage pretty effectively.

One of the primary challenges in prosecuting Internet-related crime is that exposure in numerous jurisdictions is the norm, not the exception. Prosecutors who have usually only prosecuted cases of crimes committed in the jurisdiction they serve are now faced with victims, perpetrators, or witnesses who may reside in another state, or even another country. It may be fairly easy to decide to prosecute a perpetrator who stole $50 from 100 people in the same jurisdiction. Given the amount of $5,000, it would likely be a felony. But, how do prosecutors deal with a perpetrator who stole $50 from 100 victims but only one of those victims is in their jurisdiction? Which of the individual prosecutors' offices, given their limited resources, is going to pursue the misdemeanor committed in their jurisdiction?

The panel touched on the pragmatic concerns of the elected state attorneys general, for whom they (and the members of the audience) worked. Specifically, what is the interest, other than the general pursuit of justice, for an attorney general's
office to pursue a defendant where no victim resides in that jurisdiction? TERRY BERG commented:

The problem becomes: what is the interest, if you will, or how strong is the interest of the prosecutorial entity when there's no victim, when there's no harm occurring in the jurisdiction of that entity? Now that's a harder question, I think, for county prosecutors than it is for an attorney general's office, because then you have the whole state.

While the incentive to prosecute may be greatest in the jurisdiction where the victim lives, from a practical, judicial economy line of reasoning, TERRY BERG believed that it may be most effective to prosecute the case where the defendant resides:

Generally speaking, the proper forum for the prosecution is the location where the defendant is, not necessarily where the victim is located. That's where the police are who can effectuate the arrest. Where the defendant is, that's where much of the evidence will be located.

Where the defendant is, that's where the physical crime occurred, whether it is typing on the computer or sexually abusing someone. So, the proper venue is usually where the defendant is located.

A criminal investigation and prosecution for criminal activity that takes place in numerous jurisdictions is always challenging. TERRY BERG shared an in-depth example of a case involving a great number of victims and how this can be handled when the crime is very "widely spread" out:

We had a case recently that was the enforcement of what's called the CAN-SPAM Act.\textsuperscript{5} It's the federal

Anti-Spam statute. Do any of you have state anti-spam statutes? I know a lot of states do now, with criminal, as well as civil, provisions.

Well, if you’ve done any of these cases, you know that they’re very difficult in terms of how widely spread [out] they are. That’s one of the key characteristics about them. Let me take a minute here and tell a little bit about [one] case. The defendant’s name was Daniel Lin. It began with the Federal Trade Commission, which does a great job with their investigations. They had received a [number] of complaints regarding spam advertising medical products, various different medical products you see advertised on the Internet, including these diet patches and Viagra—they were selling Viagra that was manufactured in India. They were selling pills that were to enlarge certain portions of your anatomy. They were selling things like that. At any rate, there were all sorts of complaints. The question becomes, “How do we find out who is doing this.”

As you can imagine, the method [the investigators] tried to use was [to] follow the money. They made some orders. Then they tracked where the money was being paid. They were able to determine that it was essentially being deposited into the account of an individual who was in Michigan.

In a CAN-SPAM violation case the issue is, as you know, “Okay, who’s actually sending the spam?” not necessarily “who’s benefiting financially from the purchases that occur when somebody who clicks on the spam goes to the website and makes a purchase.”

So, you have a commercial connection but not necessarily the answer to the question of who is sending it. So, as the case developed, what we found out was that these folks were using “open-proxy computers.”

Essentially, a proxy computer is just a computer that’s on the Internet that other computers connect to for the purpose of going to the Internet. A lot of corpo-
rations and the government will have a proxy computer that when you go to the Internet you actually go to the proxy computer, and it is that computer that actually takes you to the Internet.

Well, if these proxy computers are left open, then they become like relay stations that the spammers use. They look for those open proxies. There is a whole black market for lists of open proxies. That’s what these folks were doing in this case.

Fortunately, through the help of some of the victim’s groups, we were able to make some headway. I think victim’s groups can really be helpful in this area. There’s one called “SPAM HAUS” that was able to essentially connect the investigators to a company that was in Germany that was running what they called a “proxy pot.”

A proxy pot is a computer that’s sitting on the Internet looking like an open proxy so that when individuals who are either selling the proxy lists, or otherwise just looking for open proxies by doing scans, they will find them. They find that set of IP numbers that appears to be an open proxy.

Then when the spammers go to do their blasts of spam and they send it to all these different open proxies, they actually sent it to this proxy pot that was located in Germany. So, once we were able to get the information from the company in Germany, we had the advantage of having the connection where the spam was actually originating from.

The reason they use the open proxies in the first place is that it hides the origin of the computer transmission. It looks as if it’s coming from the open proxy computer, rather than from the person who’s actually sending it.

So, with the help of the German company (the proxy pot company) we were able to determine who the actual “button-pusher” was. Who was the person actually sending the spam in this case?
This was because the company was logging all this information. That was the whole point of the proxy pot. That enabled us to say, "Okay, this is the person who is doing it?" This brings to light a number of different points about victims in this type of case.

If you think about a spam case, it is almost the epitome of a computer crime case. It brings into play all of these different questions and problems as it relates to victims. The one point is [that] if you look at what cracked the case, it was the German company with the proxy pot that enabled us to say, "Okay, now we can track back to Daniel Lin and his cohorts who were sending the spam."

So, the company is actually a victim. That's a cooperative victim, because that proxy pot was sitting out there on the Internet, just like all of those other open proxies, but it's just that they were intending to be a part of it. Then the spam went through. This is one type of victim.

The next question, which we also have in other Internet cases, for example, fraudulent website cases, auction fraud cases, etc., is:

"Okay, who is the victim?" How do we determine who the real victim is in a case like this?

The victims could come from lots of different places. They could be the individuals who purchased the products, which would be the quack medical products that don't actually work, and so they are out money. In this type of scheme there are going to be a lot of people who fall into this category. How do we determine who they all are?

That's one way of looking at it, from a consumer fraud angle. The other way of looking at it is [that] every single person who received the spam [is a victim]. That's getting to the point of being impossible to
keep track of since this spam was going out at rates in the millions of emails.

So, from this angle you are talking literally millions of possible victims. Another type of victim would be the ISP’s, your Internet service providers who may have been in some way or another damaged by the fact that they received all this spam.

So, it was a very difficult question in terms of who the victim is in a case like this. Because, at least in the federal system, and I'm sure it's true in states too, there's a very serious regime of laws regarding victim/witness relations [among] the government and the victims that involve things like notification.

If you’re going to take a case and say that as part of the case you have several million victims, does that mean that you're going to take the responsibility of contacting all these victims, telling them what court dates there are, making sure they have an opportunity to talk to the court at sentencing?

So, it becomes very, very difficult. In our case the way we dealt with it was almost by punting and saying, “we’re not really going to consider all of these people that received the spam or even purchased the product as being the victims” because we did not have quantifiable financial losses.

Instead, rather than trying to accumulate the loss amount for sentencing purposes through that method, we simply looked at how much money was [the defendant] actually making because the federal sentencing guidelines allow us to use “gain” when loss is hard to determine. So that was kind of how we dealt with it. I just wanted to give you that as an example of a case, and try to address that.

In addition to the value of task forces, another area that there was unanimous consensus among the panelists was the advantages that come with cross-designating a state assistant attorney general as a Special Assistant U.S. Attorney. PRO-
FESEOR CORBETT expanded:

[Assistant attorneys general] should consider getting Special Assistant U.S. Attorney status. It is something that can really put you in a unique position to be able to make the case. If you've got the monetary threshold met and you're working with a task force like so many people have talked about already, and you've also got the Special Assistant U.S. Attorney status, which is something you get by working with the U.S. Attorney in your federal district, you're in a position where you can take the case.

You can be the one that takes it into federal court. Or, you can take it into state court. Whichever jurisdiction works the best, consistent with what you, as part of a task force working with the federal or state or local officers, have concluded is the best way to go.

As a practical matter in obtaining such special status, TERRY BERG observed that it should be for a specific case or series of cases and not just a general designation. He added: “If you're going to do that, try to make sure that you have an [actual] case that you want the person to work on.”

TOM SADAKA provided a final example of the effect that different jurisdictions or districts can have even within the federal system:

Of course the real fun is when you start ending up dealing with multiple districts. We had an identity theft ring that we chased up into Georgia [from Florida] and made the arrests in Georgia. The case was handled by federal prosecutors in Georgia. One brother pled out to five years in prison with the agreement that he testified against the other.

The other was successful in getting his case transferred to the Southern District of Florida, [where it was] promptly dismissed it because it was below their million [dollar] threshold.
A final comment on effectively dealing with large numbers of victims and the inevitability of multiple jurisdictions was offered by TODD LAWSON who expanded on how large numbers of victims create notification problems:

Most of our big victim cases, when it gets over into the something hundred range, we haven’t even necessarily been able to contact them all. Usually in those circumstances we’re finding the victim’s information in the possession of the defendant after execution of the search warrant.

Only in the rare eBay case do we have all the victims talking to us. Even then, by the time we do get around to arresting the guy, 30% of those people have moved on or don’t want to deal with us anymore because we’ve taken too long. In a number of our cases, the first contact with the victim is when we send the victim notification letter to say, “Hi, you’re a victim.”

QUESTION 3:
What role does the characteristics of Internet victims or their experiences play in the decision whether to prosecute?

The panel examined the characteristics of the crime and the particular victim or victims when “triaging” a case and making the decision whether or not to proceed. TERRY BERG stated the question this way: “What kinds of cases involving what types of victims should get priority?”

Some of the characteristics discussed prior to the panel were:

• seriousness of crime/victimization;
• ease of victim identification;
• chance of recidivism with the same victim (e.g., incest, etc.);
• age of victim;
• previous instances of victimization;
• ability of victim to testify adequately;
• credibility/perceived character of victim;
• whether victim is a "persistent" victim (with regards to past claims);
• trauma to victim from testifying in court;
• "politically-connected" victims; and
• existing or anticipated press coverage of victimization/victim.

One of the most prominent characteristics that emerged as being relevant in the decision to prosecute is whether crime involves a "real child victim." "For instance, in your child exploitation cases, try to focus, if possible, on those cases involving real child victims, whether being exploited sexually or just simply being the subject of child pornographic pictures."\(^6\)

The panel considered not just characteristics in the affirmative, but also in the negative, in terms of "red flags" that might cause hesitation on the part of a prosecutor to accept or pursue a particular case. One such "red flag" identified initially by TODD LAWSON is where the victims have themselves retained legal counsel: "I'll tell you the number one thing that I do not like to see are lawyers. If victims have lawyers, I immediately step back. If defendants have lawyers, well, that I've come to expect."

This "red flag" often occurs in cases involving corporate victims, as TODD LAWSON continued:

I have had one occasion, where it was an organized crime kind of thing where the defendants had a business front. The victims were so numerous that one of them was a lawyer and the lawyer has whipped up the other victims into fervor and they have started to talk about going class action lawsuit.

Then somebody says, "Hey wait. Let's call the criminal attorneys." I say, "No, you go run with that. You take care of that on your own." If the victims have

---

\(^6\) See supra note 3 (paraphrased version of conversation among Panelists and Moderator).
enough money to hire their own lawyers, they probably have enough money to seek their own civil recourse. So, we generally step away from those [cases].

PROFESSOR CORBETT continued on this topic, relating his experiences that crossed-over between his time with the attorney general’s office and his time as a law professor. Specifically, Patrick Corbett articulated the importance of gauging the victim’s motivation in turning to law enforcement:

Two quick stories related to the issue of dealing with the corporate victim. When I worked for the attorney general’s office, we’d receive calls like this and since I’ve been a professor, I’ve received calls from attorneys on behalf of businesses.

Generally, the claim is that this former employee hacked into the computer system and we’re bringing the case to you. We’re representing the corporation and we’re bringing the case to you to go ahead and prosecute it for us.

Well, I still remember vividly having a lengthy discussion with this attorney from the Detroit area working for [a] silk stocking firm. He’s going on and on with the IT person there talking about how bad this was, and this employee was really out of control.

Fortunately, we took some time to think about it; because it turned out they were involved in a serious labor dispute. The employee sued the corporation. He ended up winning. The corporation ended up paying out something like $500,000.00 in a suit. You have to be really leery of that.

Just to give you another story, I’ll periodically get calls from corporate attorneys and criminal defense attorneys at the law school. I had this one guy calling up and he’s representing this business.

He says, “So, I’m wondering if you can help me figure out what statute would be applicable, and which law enforcement entity I should call to get this case pursued?” So, I’m going through it with him. I’m
thinking, “Well, it sounds like you might have some problems with your case with regards to whether or not the access was wholly unauthorized. That’s always a big barrier. Do you have employment agreements or acceptable use policies, things like that? That’s what law enforcement is going to be asking you about.”

We talked for about a half hour, forty-five minutes, and got to the point where I said to him: “I’m a little worried. I just have to ask you this question. Why is it that you want to contact law enforcement?” He told me directly that he’s looking to gain a civil advantage in his lawsuit. Came right out and told me that. You always kind of assume it but this guy told me flat out.

That’s what it boils down to. If you think you’re being contacted for the civil advantage of the case, or a corporate-type case, that’s the caveat. It’s not just that you’re being contacted by a lawyer, it’s that you’re being contacted for the purpose of them utilizing your office to gain a civil advantage.

TOM SADAKA emphasized that the fact there is a lawyer involved, or a lawyer contacting law enforcement for assistance, does not necessarily mean that the motivation is to gain advantage in a civil case. He shared another experience:

I’m working with a company right now. We found a whole load of child pornography on their system. I’m going to call a prosecutor on that case and I’m not trying to gain any civil advantage.

I want the crap off the system. It’s contraband per se. There are no exemptions or exceptions under the law. I need law enforcement to come in and get that stuff off the system. So, I’m not trying to gain a civil advantage. So, don’t just close the door because you have a lawyer who is representing a company coming in. Look beyond to see what the motivation is.

Cases where the victim may be politically connect-
ed, in the public eye, or high profile for some other reason can affect the initial decision to prosecute. Prosecutors' offices are led by an elected official and are dependant (at least in part) on the legislature for appropriate statutes and funding.

As such, certain pragmatic concerns are always present. TODD LAWSON suggested this topic and started the discussion:

For example, when we have state legislators who call, we try to give them the function of constituent service. It helps them to understand the problems faced by regular constituents. I mean, a state legislator told us earlier this year that he doesn't understand identity theft because he doesn't own a credit card.

So, there's a fundamental level with some politicians and some people who are higher profile that you do have to take their complaints sometimes just to work them through the process, even if it isn't necessarily your biggest case.

Jack [Christin, of eBay, Inc.] knows. I've been bugging him about a politician who lost $4,000.00 on eBay. But, it's not a big case. It's probably never going to be a big case because our bad guy is in Chicago and he's pretty good about hiding himself. But, it does help to kind of walk them through the process of what help a victim can get, it helps us and it helps them understand better.

The other thing we do [in relation to high-profile and public cases] is we just watch the papers and watch for cases where there is an Arizona angle or a place where we can step in and help. It just makes your agency more responsive to the needs of the public and kind of helps you out in the court of public opinion, which helps you at the legislature.

So, they're not the biggest cases. They're not your most important cases. But, sometimes they're the ones...
that get you the most mileage in other ways.

PROFESSOR CORBETT offered insight into a situation where the perception that certain crimes were reaching “epidemic” proportions made the entire community a type of victim and, because of this exposure and publicity, the decision to prosecute was affected:

I just have a quick comment on a case that occurred in Michigan that I think fits with this concern [very] well. In this case, there was a kid in Michigan who was communicating with a kid in Washington state through a chat room. The chat discussions revealed that the Michigan student planned on doing some bad things. It turned out that the kid in Michigan had a treasure trove of firearms and guns. Law enforcement did a search and ended up arresting the father and the son. This case was a pretty big deal in the area of Macomb County, Michigan.

This same school district [Chippewa Valley School District] has had some more problems related to stalking and problems with teen use on the Internet. A seventh-grade, 13-year-old using [AOL’s] [I]nstant [M]essenger (IM) to communicate with her friends and some people that go to the school, had basically threatened to blow up the school.

For these threats, she was prosecuted by the Macomb County prosecutor's office using a 20-year [sentence] anti-terrorism felony that was passed by the Michigan legislature in 2002, shortly after 9/11. They're doing this for the deterrent effect, the fact that there's this huge amount of community interest in it. It has, I think, had some significant effect, because a lot of different parents and educators that I have spoken with have heard about this case. They talked to their students and kids about it. So, there is some value in doing it from that type of perspective.

Who's the victim here? Well, it's the school dis-
strict. It’s the community as a broader matter. So, there’s some value in taking a case like that. Sometimes it is purely for the deterrent effect. We can, of course, question whether or not a 12-year-old sending instant messages is the right defendant for an anti-terrorism law and there is some head scratching that goes on there. But, that being said, clearly it’s serving a function.

TERRY BERG expanded on this idea related to the public’s perception that certain crimes (i.e., Internet ID-theft, school shootings, child pornography, etc.) have “suddenly become something extremely serious or of an epidemic proportion.” He added:

The question relates to when you have a case or a series of cases that in the perception of the public have now suddenly become something extremely serious or of an epidemic proportion.

Whether it’s in the case where the minor has used the Internet to threaten a Columbine-type of act in a high school or a number of smaller incidents that we’ve had in my state where students have expressed threats, even in one case on a bathroom [wall] which resulted in very immediate and “robust” law enforcement response in terms of charges against the minors who were involved.

I think it is a combination of a lot of pressures that we’re talking about here. You have the question of the vulnerable victim—these are children that are in a school situation. Then you also have the public perception of danger associated with any Columbine-type of crime which, obviously, law enforcement and [the] community wants to make certain never happens again.

I don’t really know the answer to a question like that. We had some questions from the press to our office about [one of the school threat cases]. I could tell
from the question that the person asking [was] fishing for a response like: “Well that’s an overreaction. We don’t necessarily . . . .” Of course, I was never going to say anything like that, because frankly I can’t say that it was an overreaction [where] you have a situation where there is an actual threat of attack on school children.

Of course, law enforcement has to take it seriously and respond. But, it’s a difficult juggling act. Before Columbine, it is likely that many of these cases would have been treated with only an interview to determine whether there was an actual threat. In many cases, law enforcement would not have been directly involved, instead it would have been handled administratively and internally at the school.

Collectively, from the comments above (and some made by the audience) it became clear that, in many cases, prosecutors felt different types of pressures based on politics, public or media interest, or other factors, which could, in turn, influence the decision to prosecute. In some instances, where the community expressed interest or an expectation in a certain matter, the community as a whole becomes a distinct Internet victim that warrants consideration.

Of course, pragmatic concerns will, in many instances, have to yield to ethical or prosecutorial duties when deciding whether to prosecute. TOM SADAKA stated:

That’s fine as long as it doesn’t then impede upon your ethical obligations to have reasonable certainty of convictions when you file the case. There are a number of times where the political pressures try to get you to file on a case that you know you can’t prove. Or at least you can’t prove it the way that it is charged. That’s really where the separation is. You can accept the pressure, but stand by your ethical obligations.
QUESTION 4:
What are the policies and procedures related to case acceptance or denial?

One question that was posed to the panel related to policies and procedures related to the decision to prosecute. The moderator posed the question this way:

We’ve pretty much been talking about all these things from a very subjective, discretionary point of view. But, fairly quickly, what mechanics, policies, and procedures are there relevant to these triage or charging decisions? And then what role does the victim play? Does the victim play enough of a role or too much of a role from your experience?

One procedural consideration that was mentioned by TODD LAWSON was whether or not he has to list a particular victim:

I’ve already referenced one tool that I use in terms of mechanics of the decision, [which] is I like counts where I don’t have to name the victims. I like the ones that give me expandability where I can have five people testify in support of it, or, in theory I could have 228 testify in support of it.

So, sometimes it’s the charge you select, and the requirement that the charge identify a particular victim in its text. Whereas, there are certain advantages if you can just attach a victim to a group count.

TERRY BERG provided an in-depth examination of this question. While his answer primarily addressed his opinions in the context of the federal system, the interesting hypothetical has broader application and is helpful to state prosecutors as well:

There are also cases where you have a victim who
presents problems. The troubled teen victim in your child exploitation cases would be an example. For instance, a case where the scenario is that the defendant is an individual who's himself close to being a minor—let's say around 19 years old—is chatting with a minor female on the Internet in a sexually inappropriate manner.

Let's say the defendant has a very dark personality on the Internet. He's posing as a person who does contract murders and he's just an awful person. This teenager victim is actually chatting about possibly having this person kill her parents. So, this is obviously a very troubled teen.

As the chat continues, this develops and it becomes your typical solicitation situation and the defendant solicits the minor to send pornographic pictures of herself, which she does and gets her friend to do it as well. In this example, you can see that you have a very troubled person who is also a victim.

So, then the question becomes: "What's the proper thing to do. How do you deal with a case like that? What's the proper way to charge it?" For example, in the federal system there are mandatory minimums that apply in child exploitation cases. For production of child exploited material or child pornography, you can get between fifteen years as the minimum and thirty years [as the] maximum.

So, that's a very big hit. Here, you're talking about a defendant who is close to being a minor himself—19 years of age. You have a production situation, which is arguably not coerced at all because of the nature of the troubled teen and the nature of proof in the case.

So, the question becomes: "Do you go for that?" "Do you give the maximum charge?" Or, "do you go to a lesser charge?" For instance, instead of being production of child pornography the defendant could be charged with transmission or receipt of child pornography, which has less severe penalties.
Anyway, I'm just bringing all that up to say that this is how I think victims come into play in the charging decision. I've mentioned some of the procedures we go through. In my office they would be all those facts I've just laid out in an attempt to determine whether or not you would give the person an opportunity to plead guilty to a lesser charge.

QUESTION 5:
*What are the challenges in dealing with law enforcement in Internet victimization cases?*

Another subject discussed was the challenges in working with law enforcement agencies in the context of an Internet crime case. It appears that many of the problems that arise are related to jurisdiction; the willingness to take the initial police report when it is unlikely any action will be taken by the reporting department; and, pragmatic issues that arise with crime statistics and law enforcement's general resistance to change.

Law enforcement agencies, for a variety of reasons are reluctant to take police reports in Internet victimization cases. In response, the Arizona, Attorney General's Office prompted the legislature to change the "I.D. theft statute to say that the [police] report can be taken where the victim lived or where the perpetrator was" according to TODD LAWSON. However, the police departments lobbied the legislature to change the law back to its original form. The Arizona Attorney General's Office again worked with the legislature and the law was changed back, again, to allow for the report to be taken where either the victim or the perpetrator lives.

Why would police departments not want to take police reports? Several reasons were discussed. The first goes back to budget. Police departments are concerned that because of budgetary restraints, they will not be able to do anything for the victim.

TODD LAWSON expanded on the situation in Arizona, exemplifying on this difference of opinion or priority:
Yes, we went round and round with [law enforcement] on that. The basic underlying principle of it was you give a guy who calls up and says, “Hey, somebody just stole a bike from my open garage” a report, why not give the guy who calls up and says, “Hey, I just had my identity stolen.” Prosecutors believe that this is very important because of how many of these cases start with a single report. The response of the police is: “Well, we can’t investigate this stuff. We don’t have the money to do that.”

One cause of this tension between prosecutors and police appears to be the expectations placed on the police if they take a report. The question arises: do you have to do a follow-up investigation on every police report? Several audience members provided information about states that passed legislation stating that, though the police departments should take the report, they do not necessarily have to conduct a follow-up investigation.

TOM SADAKA stated that a specific statute was likely unnecessary because law enforcement is generally not required to investigate every report:

The irony, though, is that it is underwritten in every criminal code that there is no obligation, maybe with the exception of child abuse, on the part of law enforcement to conduct any investigation. So why, just because you’ve created jurisdictional ability for them to take the report, or really just a clarification, because the jurisdiction really existed regardless, why do they now feel that because it says they can investigate that in this instance they are compelled to investigate? These departments have always had the ability to triage everything that came in anyway.

A second reason for police reluctance is that certain cyber crimes because of multiple jurisdictions and other factors do
not fit into the normal model for law enforcement statistics. An audience member relayed the following story related to how the manner in which clearances are indicative of job performance can make this type of crime less than desirable from a police point of view:

When this identity theft issue came up initially, the police chief was very interested in it and encouraged it and everything. So we were rolling it out and getting this particular agency involved. When the first shift lieutenant realized that his shift would have to take this type of report, he became furious about it. The reason is that they don't get a clearance right away. His shift ends up taking the bulk of the reports but he's not getting any additional manpower to pursue the reports and, in many cases, this isn't the type of crime that the agency would be able to investigate as it might only be the victim that lives in the jurisdiction, not the perpetrator. So, in time, his clearance rate goes down. He looks bad and he's demoted.

TERRY BERG commented on this point (to the general agreement of the audience) that it is "an administrative issue. They could create some kind of code on an identity theft report that doesn't factor into the clearance rating. That's purely an internal administrative issue and shouldn't factor in." PATRICK CORBETT added that, in many cases, the actions of the legislature created problems because of increased expectations on law enforcement without any additional resources:

It gets back to what the legislature's doing. They are imposing more and more new opportunities or requirements on various law enforcement entities, but generally not supporting these entities with any kind of increased funding.