MR. MALCOLM: The debate about how to strike a proper balance between cherished privacy rights and the legitimate needs of law enforcement and the intelligence community is not a new one. This debate, however, has grown more vigorous and more vociferous and, of course, increasingly more important since the shocking and unprovoked attacks on the World Trade Center and the Pentagon on September 11th of 2001.

Although it is vitally important that we do everything we can to pursue and apprehend terrorists, I do not believe that, at least as it pertains to the Electronic Surveillance provisions, the U.S.A. PATRIOT Act signals some kind of fundamental shift between online privacy and Governmental power.

There are those who believe that with respect to many aspects of the war on terrorism and also with respect to the surveillance provisions in the U.S.A. PATRIOT Act, the pendulum has swung way too far in terms of denigrating privacy rights at the expense of law enforcement and intelligence gathering. In fact, I think there are those people out there who think that the Department of Justice is essentially acting like some voracious PacMan that's running around and swallowing civil liberties at every turn.

Still there are others who believe that the Government ought to be given even greater tools to protect the public from further harm. It is certainly true that the public at large expects us to use, in an appropriate manner, all of the tools that are in our arsenal, including those set forth in the U.S.A. PATRIOT Act to prevent additional attacks and to bring to justice those who were and are responsible for plotting against us. And, speaking, at least from the perspective of the Department of Justice, I believe that we are doing just that, and I'm unapologetic about it.

We recognize though that while desirous of feeling safe and secure, Americans are extremely reluctant, as they should be, to give up their privacy. Many are understandably on guard against what they perceive as Governmental overreaching at this time of crisis. This backdrop frames much of the debate about security versus freedom and explains much of the controversy that continues to surround the U.S.A. PATRIOT Act, and I assume will be surrounding it for years to come.

This is an important debate that is healthy for a free society which is governed by the rule of law. The Department of Justice has not abandoned the rule of law; we embrace the rule of law. I applaud all of those attorneys out there in privacy groups that are challenging government actions. These issues are being trumpeted in the public and talked about in front of Congress and talked about in the courts. That's good; that's the way it ought to be.

I believe, however, that in terms of advancing this debate, there has been a lot of misinformation and hyperbole about the scope of change brought about by the U.S.A. PATRIOT Act. In addition, there are provisions of the U.S.A. PATRIOT Act that in fact protect and extend civil liberties, including increased civil penalties for improper disclosure of surveillance information and new reporting requirements when the government installs its own pen trap device such as DCS-1000, which of course was originally referred to as Carnivore. I suspect that the person who originally named it Carnivore is one of those people who, as a previous speaker suggested, is now in the private sector. A lot of these privacy enhancing provisions have been roundly ignored by the press.

While there are those who contend that the U.S.A. PATRIOT Act has dramatically expanded the powers of law enforcement, I would contend that in fact it is a very measured piece of legislation. I'd like to begin with a brief overview of the PATRIOT Act and then discuss a couple of its more controversial provisions, specifically the pen register and trap and trace statute and its application to the Internet, and the computer trespasser exception, which Chris Painter talked about a little bit.

The U.S.A. PATRIOT Act provides the law enforcement and intelligence communities with new tools and resources to prevent terrorist acts and to apprehend and punish the perpetrators of such acts. Two fundamental objectives animate its provisions. First, to increase our surveillance capacities with respect to criminals and terrorist networks. Second, to enhance our abilities to swiftly track down and apprehend criminals and terrorists, hopefully before they act.

Now regarding the Internet and other electronic communications, the Act expands existing provisions that permit law enforcement, with appropriate judicial oversight, to intercept and access communications.

The U.S.A. PATRIOT Act accomplishes many of its objectives by updating surveillance laws to account for changes in technologies that have occurred over the intervening years, such as the increased usage of emails, the Internet, and cell phones by both cyber criminals and by terrorists. In this way it updates the law by making it technology neutral.

Just because new technologies have emerged, should that mean that criminals now have some new ways to thwart legitimate law enforcement activities? By means of the U.S.A. PATRIOT Act Congress has declared that cyberspace should not be a safe haven for cyber criminals, terrorists, and others who are bent on committing criminal activity. By the same token, the same privacy protections that were afforded to users of the telephone during its hay-day, have for the most part been extended to these new technologies, too.

Now as I previously mentioned, one of the more controversial provisions of the PATRIOT Act involves the application of the pen register and trap and trace statute to the Internet. Congress enacted the pen register and trap and trace statute in 1986, and it requires the Government to seek a court order for so-called pen trap information.

Now in rough terms, a pen register records outgoing addressing information, and a trap and trace device records incoming information. For the telephone a pen register would record the numbers dialed from a telephone, and a trap and trace device would record all the incoming numbers.

In 1979 the Supreme Court ruled that in the telephone context there was no reasonable expectation of privacy in this sort of non-content information, because it was shared by the user with communication service providers. This means that from a constitutional perspective there was no court order necessary in order for law enforcement to compel production of this information.

When Congress enacted the pen trap statute, thereby providing statutory protections that were not afforded by the constitution, it did not anticipate the new communication technologies which we have today, such as the Internet. Indeed, some of the language that Congress drafted in the original pen trap statute appeared to relate to the telephone only. For instance, it defined pen registers in terms of numbers dialed.

The PATRIOT Act updates the pen trap statute's language to make it tech-neutral, as it now applies more generally to dialing, routing, signaling, or addressing information. It also makes explicit that which had previously been implicit and constitutionally based, a distinction between content and non-content.

Thus, the pen trap statute now unambiguously applies to Internet communications, which could be interpreted, by the way, as another extension of civil liberties. If something wasn't constitutionally based and the original statute didn't apply, arguably law enforcement didn't need any kind of a court order in order to get this information. Now the pen trap statute clearly applies to the Internet. Clearly you have to get a court order.

However, the pen trap statute's new language does not constitute a significant expansion of Government power. In fact it's hardly an expansion at all. Prior to the U.S.A. PATRIOT Act, the Government was already using the pen trap statute, adopted almost universally by every court to consider the issue, in order to get non-content information in many jurisdictions. The PATRIOT Act has simply confirmed that this was a proper course of action.

Consider, for example, the case of James Kopp. You may recall that he was indicted for the murder of Dr. Barnett Slepian, who was an abortion doctor in East Amherst, New York. Mr. Kopp, who was wanted by law enforcement officials, communicated with his cohorts through a shared Yahoo account. To avoid sending emails, they left messages for each other in the account's drafts box, which they then accessed through the Internet.

Federal prosecutors sought a trap and trace device in order to get information concerning the IP addresses from which the account had been accessed. Through that information, Mr. Kopp was traced to France, and he was arrested. This happened in February of 2001, during the very early days of the Bush Administration, long before the events of September 11th and long before the enactment of the U.S.A. PATRIOT Act. Mr. Kopp has been extradited here. He is now awaiting trial.

Next let's consider the U.S.A. PATRIOT Act's computer trespasser exception, also known, as Chris Painter already told you, as the hacker trespass exception to the Wire Tap Act. This provision generated a surprising amount of opposition. A good portion of that resistance, I believe, comes from people who simply don't understand what it is.

For example, there was one senator during the debate who said that the hacker trespass exception could be used to monitor the emails of an employee who has used her computer at work to shop for Christmas gifts. This is simply untrue.

All right, so what is the computer trespasser exception? To explain, I'd like to give a very brief overview of the Wire Tap Act, which provides the statutory framework governing real time electronic surveillance of the contents of communications.

The structure of the Wire Tap Act is surprisingly simple. The statute's drafters assumed that every private communication could be modeled as two-way connection between two participating parties, such as a telephone call between Person A and Person B. The statute prohibits a third party, such as the government, from intercepting private communications between those parties using an electronic, mechanical, or other device absent a court order, unless one of several statutory exceptions applies.

Now under this general framework, as it applied prior to the PATRIOT Act, the communications of network intruders, which may be routed through a whole series of compromised computers, could be protected by the Wire Tap Act from interception by the government or any other third party. The PATRIOT Act simply enacted another exception to that rule.

The computer trespasser exception allows victims of computer attacks to authorize law enforcement to intercept the wire or electronic communications of a computer trespasser. It includes several significant limitations which ensure that it does not expand beyond its core function.

First, the owner or operator of the computer has to authorize the interception of the trespasser's communications. More importantly, the interception cannot acquire any communications other than those that are transmitted to or from the computer trespasser.

Finally, the exception may not be used when the party that's going to be monitored has an existing contractual relationship with the owner or operator of the computer. They may be going beyond the extent of that authorization, that contractual limitation, but if they have an existing contract, they are not an outside hacker. Therefore, an entity's legitimate customers and employees can't be monitored under this exception. In sum, the statue was crafted carefully to ensure that the government is only monitoring outside trespassers.

Now, although narrowly confined in scope, the computer trespasser exception is a significant new tool for law enforcement. For example, weekly we read about successful distributed denial of service attacks on computer systems all around the country. Typically these attacks are channeled through zombie computers that have been compromised and which are owned by innocent third parties.

The computer trespasser exception gives law enforcement the ability, with the consent of that innocent third party, to monitor the communications through their computers. Now some have criticized the computer trespasser exception as somehow restricting the judicial role in investigations. You've heard a lot about that.

It's true that without this exception, law enforcement would have to make a probable cause showing before a

magistrate before intercepting a hacker's communications. However, I believe that the hacker trespass exception again strikes an appropriate balance between privacy and law enforcement.

When a citizen finds a burglar in his basement in the middle of the night, he wants to protect his family, find out who this person is, and why that person is there. When that citizen calls the police, he wants and deserves immediate action. By being able to act immediately, the odds of the police catching the burglar before real harm occurs goes up dramatically.

When the law enforcement officer gets that call, he has no need to wake up a prosecutor or judge in the middle of the night in order to get a warrant. The burglar has no right to and no reasonable expectation of privacy to prowl in the middle of the night in someone else's basement. The same is true in the online world.

A computer hacker who is acting without authorization has no right to and no reasonable expectation of privacy in routing around in somebody else's computer system. Just as there was no need in the real world example to wake up a prosecutor and a judge, there should be no need for a prosecutor and a judge in the online example. There is no legitimate privacy expectation that would be served by requiring a court order and judicial oversight in this situation.

Moreover, just as it's impossible to tell who's in the basement, when a computer hacker enters into a sensitive network, it's impossible to tell whether that hacker is a script kiddie who wants to do something malicious, route around, maybe deface a page, or something like that, or whether we are talking about somebody who is a serious cyber criminal, or a cyber terrorist, who is plotting an attack, who is trying to get valuable critical infrastructure information to create a threat to life and limb.

Under these circumstances, time is of the essence. By being able to act immediately, the chances of finding out who that hacker is, what that hacker wants to do, and catching that hacker increase immeasurably to prevent real harm both to the immediate victim and also possibly to others who might be harmed by that intrusion.

In conclusion, I want to say that I think it's entirely appropriate following September 11th to ask questions about the balance that has been struck between privacy and law enforcement and security. It's entirely proper to ask such questions. I think it's great.

However, I think the U.S.A. PATRIOT Act demonstrates that, at least in the Internet context, what was needed was simply a tune-up. It wasn't a major overhaul. Congress updated the statute to accommodate for new technologies and new situations. It did so in a manner which remains faithful to old principles and long-standing constitutional doctrines.

The debate about privacy versus security is not likely to end any time soon. These are difficult times, and difficult questions that we face. Nobody should claim to have all the right answers, because none of us is omniscient. It is entirely appropriate that we have debates like this in symposiums, in courts of law, and within the Executive Branch and also in our dealings with the Legislative Branch.

Obviously there is going to be oversight. A lot of these provisions are sun-setted. We have people like Larry Thompson who go up to the Hill on a regular basis to report on these things. There is judicial oversight. We'll see where this goes.

Thanks for inviting me. I'll be happy to take your questions.

MR. CLARK: Thanks. Drew Clark, National Journalist Tech Daily. At presentations such as this it's natural that the Justice Department would want to put the most favorable interpretation of legislation on the table, and you have done that and I appreciate your tone. I just must ask, all of the things that you didn't mention, the things such as the secret searches that are now enabled and not sun-setted. For example, I guess the most important piece about which I'd really be interested in your reaction, is the changes to the Foreign Intelligence Surveillance Act, and how that opens the door to new expansive searches of individual citizens without probable cause to believe they have committed any crime whatsoever, and indeed the opening up of third-party and educational records under the FISA provisions that are now possible.

MR. MALCOLM: I've got to write down the ones you've asked me about. Hold on a second. Go ahead.

MR. CLARK: Yes, there are some privacy provisions as you point out in the statute, but I guess I feel compelled to point out each of those provisions you mentioned were the result of a legislative compromise that was not originally proposed by the Justice Department. The Carnivore reporting was Mr. Armey's insistence. Changes to the computer trespassing were narrowed because of Senator Leahy's objections. So I guess I raise that to point out that yes, it's notable as you point out, it's important to have this debate, but these weren't suggestions the Justice Department came forward with. They were only added at the insistence of Congress.

So any reactions to those points that I've made?

MR. MALCOLM: I'll react to all of them. I'll take your last one first. We live in a system of checks and balances. That's great. We have two major parties, multiple other parties, three branches of Government — Federal system and the state system — and they're all supposed to be questioning each other. They're all supposed to be looking at each other. Things are often a series of compromises.

If you were to look at the Administration's original bill, there may be certain provisions that you thought were way over the line. I certainly think there were good justifications to support all of those provisions. Did they get compromised? Sure. Did they get weakened in some instances? Probably. Did they get strengthened in some instances? Probably. Did some ideas originate within the government? Yes. Did some ideas originate within Congress? Yes. Did some ideas originate within privacy groups? Yes. That's good.

I don't think, though, that it's an accurate characterization to say that after September 11th, the U.S.A. PATRIOT Act was drafted by the government as some kind of Christmas tree that was going to go and steam roll across the country as a complete wish list of Government actions. I think that it was

tempered by Congress as it deemed appropriate. That's the way our system operates, and I see nothing wrong with that at all.

I don't think it's accurate to somehow say "Well, had it been up to the Executive Branch, the Constitution would have somehow been done away with, and it's only Congress that saved it." I think there was a lot of give and take in the PATRIOT Act.

With respect to so-called sneak and peek searches, the idea that you can go in with a court order, not knock and announce your presence, but go in secretly, search for something, or implant a device, is not terribly new.

There are Title III orders (Title III has been around for a long time), for instance, in which you get a court order to go in and plant a bug, say to go plant a bug in a mobster meeting room, that takes place under cover of darkness. People don't know that an agent has been there. They don't know an agent has left. Hopefully they don't find the evidence that indicates that an agent has been there.

All this does is apply this mode of operation to the search context. Sneak and peeks have been done in the drug area for a long time. So I think this is really a clearer codification of what was existing all along. I don't think that there's anything particularly novel about that. A lot of times you need to go in somewhere where a crime has occurred or is being plotted and get the best information that you can. But it's not an appropriate time to bring down an investigation. You want to develop leads. There's judicial oversight there.

It's not as if United States Government agents are knocking on the door or breaking in at night without any kind of oversight. All of these situations involve going in front of a judge and saying why you believe evidence is there and why you believe you need to get in there, and why there is a need to do this secretly and not to leave a sign, a calling card, that you've been there. So there's appropriate judicial oversight to that, and I don't think that it's a particularly new law.

With respect to the FISA Court changes, I assume you are talking about the balance between law enforcement and the intel community — to those of you who may not know what we're talking about, and of course if you were referring to something else, let me know — the FISA Court is the Foreign Intelligence Surveillance Court. It's a special court that sits within the Department of Justice that enters orders in cases involving — not necessarily terrorists, it can involve terrorists — but it can also involve espionage. It involves foreign powers and agents of foreign powers conducting something of interest to the intelligence community.

The FISA Court orders do not have a lesser showing to make; they have a different showing to make than one would have to make before a judge in a criminal case in which you need to show probable cause that a crime has occurred and probable cause to believe that evidence is in a particular location.

The FISA Court rules, which are set forth in the Foreign Intelligence Surveillance Act, had a provision that said that if you got a FISA Court order with this sort of surveillance by a FISA Court judge, that the primary purpose had to be for intelligence gathering. It didn't say that there couldn't be some correlative law enforcement purpose, but that the primary purpose for the order was for intelligence gathering. It was designed to separate the intel side of the house from the law enforcement side of the house.

The showing that had to be made had less to do with whether or not there was a crime being committed. Frankly, some of the stuff may or may not be a crime, but you're going to gather intelligence to see whether or not somebody is harming our national interest, that is the showing that you had to make by probable cause was that there was a foreign agent involved or a foreign country involved or an agent of a foreign power. So you still had a showing to make, and there was still a judge there who determined that.

The FISA Court statute has been amended to change the word primary to significant. The law enforcement and the intelligence community have always worked to some degree together in the FISA Court context. However, you could now have a situation in which a law enforcement objective is the primary reason to go to a FISA Court, and regarding the intelligence aspect of things, there's a significant purpose for it. It doesn't have to be the primary reason. There are a lot of people who are very concerned about a weakening of this wall of separation between the intel community and the law enforcement community.

There's only so much that I can say about it, because the matter is currently in litigation before the FISA Court Appeal Board. For the first time in the history of the statute such an appeal has been taken, and there was a court order issued by the FISA Court questioning the legitimacy of this change. I guess my response is (1) it's a change that Congress made; and (2) this was not hidden. The purpose for this, at the time that Congress considered it, was all within the Congressional record. I suppose the major reason to justify this change is because the lines in the terrorism context and the times we're facing now between law enforcement and intelligence gathering have largely blurred. They've blurred for several reasons. One, we had a shocking revelation that there were intelligence failures prior to September 11th. There are people out there now who are saying "Why didn't you connect the dots? There were signs out there that you should have read, and if you had read them, disaster might have been averted." Well, I don't know whether there were enough dots out there in order to avert a disaster. That's one of those unknowable questions.

However, it is true that we need to do a better job about connecting dots. We've literally had situations, in which the intel community was gathering information about potential terrorist attacks, which of course involves criminal acts as well, and you had the criminal law enforcement community within the context of grand jury proceedings, which are secret proceedings, gathering information about criminal activity that could implicate a terrorist attack. The two sides weren't talking to each other.

We need to find a way to get them talking to each other. In addition to that, the lines are blurred because people now realize that law enforcement, stopping people and arresting people, can be a legitimate tool in intelligence collection in the same way that intelligence collection can be a legitimate tool to aid law enforcement. It is a change. I don't think it's a dramatic change. It's a change of emphasis. The matter is in litigation. Those are the reasons for the change. You can agree or disagree with them.

I believe you also talked about records searches. I assume that mostly what you are concerned about are library searches. Is that fair?

MR. CLARK: Yes, but I think it's broader than that.

MR. MALCOLM: It is broader than that. I'm not completely familiar with all of the parameters of this. Please forgive me, but I will tell you what I can tell you, which is I don't think that there's any secret that after September 11th it was discovered that a lot of these terrorists, Mohammed Atta and the lot, did a lot of communicating in libraries on the Internet. They're there; they're accessible; you can use them and remain relatively anonymous. I think it is safe to say that libraries contain useful information for law enforcement in both criminal investigations and terrorism investigations and also for the intelligence community.

There is obviously a high degree of skepticism about law enforcement activity involving libraries, because a lot of legitimate First Amendment protected activity takes place in libraries: what you read, what you look at. The overwhelming majority of people who are there are there for perfectly legitimate purposes, and it shouldn't really be anybody's business what it is that they're reading.

I hear you. I'm with you. I also understand that there is a history of FBI abuses to some degree in that area. There were references to the 1960s civil rights era in which FBI agents were keeping files on people who were engaging in First Amendment-protected activity that was somehow unpopular within law enforcement's counter intel program. That's part of the FBI's history. We don't want to forget the lessons of history.

The guidelines that are in place for library searches reflect a recognition of that history and a wish to avoid repeating that history. One, an FBI agent can't just go in and get these records. He again has to go to a FISA Court judge or a designated magistrate, make the appropriate showing, and get a court order.

Before you ever get to a FISA Court, the FBI guidelines in this context require approval, several levels up the chain. They make very clear that there have to be legitimate law enforcement or intelligence purposes to get this information that is not protected by the First Amendment. You've got to show that there is some real likelihood that there's going to be something there showing nefarious activity that can harm our national interest in a very serious way.

So is that something to be watched? Yes, it's something to be watched. Should there be oversight over that? Yes. But there is quite a bit of oversight built in to the system that's now been changed, and let's hope that those tools are used appropriately and that they won't get abused.

MR. CLARK: Why isn't the Justice Department responding to the House and Senate Judiciary Committee request for information about oversight if there is oversight, and you expressed the desire that there be oversight? Why aren't you responding to those requests?

MR. MALCOLM: I didn't express the desire that there be oversight, but I think it's perfectly legitimate to have oversight. Actually, no, I think it's a good thing to have oversight; of course it's a good thing to have oversight.

I think that's painting with a broad brush to say that the Department is not responding to requests.

MR. CLARK: That's not answering the question.

MR. MALCOLM: Well, wait a minute. I think that's painting with a broad brush. There are, as you know, many, many subcommittees within Congress. All of the Senators and the Representatives in the House have all been elected. They're all important people; they all have a right to ask for and get information.

On the other hand, there's a lot of work to be done. The Justice Department's got a day job, too, of catching criminals and fighting terrorism. If every Congressman or Congressional subcommittee is asking for information, there's a lot of duplication that is going on. Not to mention the fact that a lot of the information that's being requested is classified. There are certain subcommittees that are set up specifically to deal with classified information.

So, one, there are appropriate channels to funnel information to Congress, appropriate subcommittees. Just because one subcommittee is upset about the fact that it's not receiving information does not in fact mean that that information is not being relayed to Congress. Part one.

Part two, there are, as you know, and this is nothing new, legitimate disagreements of opinion about what is producible. Congress has its view of Executive privilege and the President's constitutional prerogatives. The Executive Branch has its view about internal deliberation and Executive privilege material that should not be turned over.

It's not unique to the area of terrorism. You see this for instance in the fight over judges. Ask Miguel Estrada about whether or not his memoranda from the time that he worked in the Solicitor General's office ought to be turned over to the Senate Judiciary Committee. The Executive Branch has taken the position, as have a number of Solicitor Generals, both Democrat and Republican, that this is internal deliberation material and in an Executive Branch context and should not be producible under the Separation of Powers Doctrine.

The same debates though apply with respect to intelligence and law enforcement. I don't think that it's fair to say that the Administration is somehow sticking it to Congress. We are working with Congress to see to it that Congress can satisfy its legitimate oversight activities while at the same time doing the job of protecting our country and also protecting the Executive Branch. It's not just for this administration; it's also for future administrations.

MS. KAPLAN: Hi, I'm Kathleen Kaplan from Howard University. One of the things when you were talking that came to my mind was this information overload. As a lowly professor at Howard, I get 50 to 100 emails a day, which is like reading a book every single day.

MR. MALCOLM: Tell me about it.

MS. KAPLAN: So, is some of the problem just information overload with catching these cyber criminals and other types of criminals. Where you get so much information, how are you going to determine what's important and what's not?

MR. MALCOLM: I don't know. I'm not 100 percent sure I know what you mean, but let me try to tackle what I think you mean. It's a difficult question. We're being bombarded with information. I have the greatest sympathy for people, for instance, who say "Okay, we're going to raise the level of alert status from yellow to orange. But they're non-specific threats; we can't tell you when they'll occur, and we can't tell you where they'll occur or if they'll occur at all."

What do you do in response to that? I understand that. It's difficult to process that sort of information. It's a little bit, however, a situation of (1) there are a lot of people out there that are seeking that information who get very upset when you don't give it, and (2) there's a little bit of a damned if you do and damned if you don't.

If you give the information, you're accused of panicking the public and overloading folks. On the other hand, if you don't give that sort of information, and God forbid something does happen...let's face it, we live in perilous times. We have enemies abroad. There are soldiers fighting now. We have enemies within our borders, terrorist cells, people who are bent on our destruction, living right here within our shores.

If you don't give that information and people don't act in an extra vigilant manner and take whatever precautions they want to take, they avoid taking an unnecessary flights or a trip or what have you, then they'll say "You mean you knew that and you didn't tell us about it?" It's tough.

We live in a time of instantaneous news. You can get it over the Internet from any number of channels. You can get it on cable TV from any number of sources. A lot of us are news junkies. How you take that information and process that information, we all struggle with that. I get more than 50 emails a day.

The public has a right to know about it. Whether you choose to tune it out or pay attention to it, that's an individual choice.

MR. FOREMAN: Frank Foreman, U.S. Department of Education. Since this is the Federalist Society, let me ask a Federalism question. More specifically for you, what are the sorts of things that the states and local governments are incapable of doing?

MR. MALCOLM: Are capable of doing?

MR. FOREMAN: Capable and incapable of doing as far as cyber crime is concerned.

MR. MALCOLM: Well, you can give an answer with respect to cybercrime and with respect to all sorts of crimes, including terrorism, including organized crime. States have certain advantages over the Federal Government when it comes to law enforcement. The Federal Government has certain advantages in law enforcement vis-a-vis the states.

In terms of crimes that are taking place within a state, there's your local law enforcement officer who's going to know the business community, those people on the ground, know the neighborhoods where criminals are acting, be able to go out on the street and have that day-to-day contact with folks, and do a very effective job of rooting out crime, much of which will be intrastate, some of which will be interstate. They can do so perfectly well without the intervention of the FBI or Secret Service or DEA or whoever, thank you very much.

However, the Federal Government has more resources that it can bring to bear in certain specialized cases. It has certain expertise that it can bring to bear in certain cases.

I'll give you a good example. It is cybercrime and it's not cybercrime. It crosses into the area that the gentleman in the back asked about before, because it involves child porn. Many of you may have heard about the CandyMan case.

The CandyMan was an email group that was distributing child porn internationally and across many, many states in this country. Now if you look at an individual group member in one particular jurisdiction, maybe you can take the idea that "Okay, all child porn is just bad period. Even if there's only one perpetrator, we're going to investigate it thoroughly and we're going to prosecute it."

However, using that as an example, you can have crime that is in fact broad ranging. In any one state the consequences may not be serious enough to justify having the state use its local scarce resources to fight that problem. They may do so because they lack the resources and don't have the intelligence to get the big picture and to realize that what's a small problem in this state is in fact a very large organization and is affecting many, many, many states.

Those are the sorts of resources that the Federal Government can bring to bear. It can look and say, "Well, you know, it may look like a small problem, but it's a small problem here, and in this city, and in Arkansas, and in Nevada, and in Utah, and in Maine. When you add it all up, it's a pretty big problem." We have the resources and the ability to look at the totality of that and to really hit these people who are perpetrating this heinous activity hard in a way in which the locals can't.

Obviously there's a big concern, which is an entirely different debate topic near and dear to the Federalist Society's heart, about the federalization of crime. One, from a constitutional perspective, and two, from a resource perspective. Federal resources are not limitless. They are also specialized, and you want to make sure that they are being used to maximum advantage. So where do you cross that line between Federal resources and state resources? When do you choose to deploy Federal resources? A lot of the time we work in task forces; we work in coordination with each other. That has to be done occasionally.

MR. FOREMAN: Is cybercrime substantially different from other kinds of crime in a way, as far as the Federal state balance would turn out?

MR. MALCOLM: Well, it's substantially different. One, in that there tends to be more expertise, although we're trying to remedy that, at the Federal level than at the state level. Two,

people who perpetrate cybercrimes have the ability to cast a very, very broad net. They can perpetrate this crime far and wide.

Let's take a simple example. Your Nigerian scam letter. We all used to get one or two of those letters. It used to be that somebody had to sit in a room, draft this letter, sign this letter, stick it in an envelope, put on a postage stamp, and send it. Then if it came back, they had to keep a file of who they contacted and how much money they got and what letter the victim had gotten in the scam.

Now with the computer, you get these letters all the time. It's easy. You draft it up online and you send it out all over the world. If you get a positive response, it goes into one database; if you get a no, it goes into another database.

So any criminal activity, if you use the computer as a facilitating device, can be spread astronomically. Well, locally the government can't handle that. It doesn't know the scope of what's out there. It doesn't have the law enforcement tools — maybe some states do, but by and large they don't have the law enforcement tools to take on that sort of activity. They don't tend to have the expertise, although we are working very closely with groups like the National Institute of Justice to remedy that as quickly as we can.

AUDIENCE MEMBER: I have a question, I want to go back to the oversight question that Drew was asking. This is really a factual question from my ignorance, no doubt, of the PATRIOT Act. When you were talking about the example of the library search, there is a perception out there, and I hope you can counter it to assure us all, a perception of the sort of star chamber quality to these matters.

You mentioned there are FBI guidelines, approval up the chain of command, but of course still within the FBI. An application made to a court that is, as you say, within the Justice Department. Who does now, is there independent focus of those decisions?

MR. MALCOLM: The Court meets within the Justice Department. The Court is made up of Article III judges, life tenured, nominated, confirmed by the Senate, a separate branch of Government. These are not people who are in any way, shape, or form toadies to what the Executive Branch of the Federal Government would like to have happen.

We live in an open society. Unfortunately, because of the dangers that we confront, there is information of a very secret nature that has to remain secret. If you tell it to people, your sources and methods are compromised. What you know is going to be out, and perhaps what is more important is what you don't know. People will be able to rearrange their plans, alter their strategies, have a greater chance at perpetrating their crimes, or to avoid detection.

If we're conducting an intelligence investigation, let's say of a hostile government or maybe even an ally trying to gain a competitive advantage or to make up for a technological deficiency. It may be economic espionage. If you have that information out in the public, you've completely defeated the purpose of the investigation.

I mean no more that you would want to have Donald Rumsfeld sitting with the Joint Chiefs of Staff holding a public hearing and taking questions about where they're going to attack tomorrow. You can't be in the position of telling people who are bent in a literal way, on destroying us where we think they're going to strike next.

So what you do is try to have appropriate oversight and make sure that due process is followed. We try to be as open as we can. There are times, however, in order to protect our national security and insure domestic tranquility, which is a constitutional mandate, that there's a need for secrecy.

MS. EDWARD: My name is Abigail Edward and I'm an Assistant State's Attorney. Let me just preface my remark by saying that I understand working in the criminal field for a very long time. In no arena that I have been in have I ever found the cooperation among and between law enforcement and prosecutors as great as in cybercrime. It is a remarkably cooperative experience.

My question is a follow up to the previous gentleman, who was asking about the Federal balance. Do you think that that Federal balance changes as you differently define cybercrime? I think that the trouble with the definition of cybercrime is that what we term cybercrime here has been Internet crime. If you conclude that cybercrime also is an attack on a computer, which is very often done by disgruntled employees, which is a purely local matter, or could be, it could change the federal balance dramatically in my view. I wonder if you have any thoughts on that.

MR. MALCOLM: Just because we have an insider perpetrating the cybercrime doesn't mean it's not a Federal crime.

MS. EDWARD: It does not have to be, but it could be.

MR. MALCOLM: With respect to many statutes, there is concurrent jurisdiction. I supposed state laws vary from state to state, but a lot of times there's concurrent federal jurisdiction. The overwhelming majority of prosecutions take place at the state and local level precisely for that reason. There's no need to spend scarce Federal resources prosecuting every crime that could be prosecuted as a Federal crime.

There are a lot of crimes that have a peculiarly local impact. I would imagine that that balance takes place at a practical, on-the-street, in-the-office, where-prosecutors-and-law enforcement-agents-are-meeting level. It's not taking place at a more theoretical constitutional level.

If you have an insider perpetrating the crime, if we're talking about a computer network, I venture to say that all the companies that are here today that earn their daily bread online, your customers don't all come from within the state.

So if you have an insider wreaking havoc, it's going to have dramatic implications to people all over the country.

* John Malcolm is Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice. His remarks were the luncheon address at the Federalist Society's Cybercrime Conference on October 3, 2002 at the George Mason School of Law.