March 1997

Computer Crimes Now On The Books: What Do We Do From Here? (symposium)

Henry H. Perritt Jr.
IIT Chicago-Kent College of Law, hperritt@kentlaw.iit.edu

COMPUTER CRIMES NOW ON THE BOOKS: WHAT DO WE DO FROM HERE?*

*Henry H. Perritt, Jr.,** Scott Charney,*** and Gregory P. Miller*****

MR. PERRITT: Good afternoon. We thought an interesting way to approach this subject is to tell you that it might be useful to distinguish two kinds of computer and crimes issues. The first kind of issue is that which is addressed by some specific statutes to which Scott Charney is going to introduce us . . . . And that kind of computers and crimes issue involves a computer as the target of the crime.

The second kind of computers and crimes issue involves a run of the mill crime in which a computer or computer-related media figures in the crime as an instrumentality or possibly a medium on which the fruits of the crime are involved, or in which a computer or computer-readable media contains evidence of the crime.

The issues overlap to some degree, but they are nevertheless distinct and, therefore, we thought it might be useful to distinguish them at the outset . . . . As we go along, we . . . will distinguish the two perspectives, and we invite you to do likewise when you think it is useful to do so.

We would like to begin by introducing you to some statutes that may or may not be familiar to you, the statutes that figure in the first category where computers are targets of criminal activity. Scott Charney is going to do that. Scott and I have worked together on panels like this . . . off and on for a number of years, and I know how effective he can be and how interesting and deep his stock of war stories is on computer crimes and computer-related criminality.

We thought an interesting way to introduce us to the statutory framework would be for him to work us through some of those problems. In doing so, he will explain not only the basic legal structure of the statutes, but also . . . why some recent amendments have been made to statutes that have been on the books for ten or fifteen years.

After he does that for ten or fifteen minutes, . . . we then want to use two hypotheticals. When Mr. Miller suggested it, I thought—being a law profes-

---

* Henry H. Perritt, Jr., Scott Charney, and Gregory P. Miller, Remarks given at the Fifty-Seventh Judicial Conference of the Third Circuit in Philadelphia, Pa. (May 16, 1997).

** Dean, Chicago Kent College of Law, Illinois Institute of Technology, Chicago, Illinois.

*** Chief of the Computer Crime and Intellectual Property Section in the Criminal Division of the United States Department of Justice, Washington, D.C.

**** President and Majority Shareholder, Miller, Alfano & Raspanti, P.C., Philadelphia, Pa.

sor—that it would be a great way to do things . . . . When we get to them, we will read them orally and reiterate the facts as necessary.

We will spend about thirty minutes on each of the hypotheticals, which should give us an interactive opportunity. Then, at the end of the program, we will take about fifteen minutes for completely free form questions, answers, and argument. I see my role as being a sort of . . . traffic cop, time keeper, and troublemaker. If it seems like we need to do something to increase the level of dispute between Mr. Charney and Mr. Miller, then it will be my job to try to make that happen.

In the unlikely event that the level of dispute between them gets too great, I guess it's my job to call for the deputy marshals or something to come into the room. Okay, Scott, . . . tell us about the legal framework.

MR. CHARNEY: Thank you. On October 11th of last year, the National Information Infrastructure Protection Act of 1996[1] was passed . . . . It substantially rewrote the Computer Fraud and Abuse Act.[2] . . . What this statute is designed to do is protect the confidentiality, integrity, and availability of computer data and systems.

That construct—confidentiality, integrity, and availability, which nicely works out to the acronym CIA—has actually been revised because we are running into all sorts of situations where we found that existing law did not keep up with emerging technology. This is because criminals were doing bad things in ways that, when you tried to apply existing law, we could not combat very well.

The way § 1030 is now structured is that under § 1030(a)(2), it is a misdemeanor offense to access a computer without authority or in excess of authority. "In excess of authority" means getting information you are not supposed to have, . . . such . . . as financial information, information from the government, or even private information if the defendant's conduct crossed state or national borders.

It is a misdemeanor to get that information, but it elevates to a felony if something is done with that information which is "aggravating." That is, the information is used for "personal or financial gain or commercial advantage," a term that comes from the Copyright Act; is used for an "illegal or tortious purpose," that comes from the Wire Tapping Statute; or if the value of the property is over $5,000, . . . the monetary threshold used in many federal statutes like interstate transportation of stolen property.

Section 1030(a)(5) is the other critical provision. That provision makes it illegal to access a computer without authority and basically cause any damage. That is, if you hack in and cause damage, it is a misdemeanor. If you hack in and recklessly cause damage, it is a felony.[3] . . . It is also illegal under § 1030(a)(5) to intentionally cause damage without authority to assist them.

---

1. Information Technology Management Reform Act of 1996, 40 U.S.C. §§ 1401-1503 (1996).

2. 18 U.S.C. § 1030 (1996).

3. Recklessness is defined here as action taken in conscious disregard of a known risk.

And that applies to both outsiders and insiders because insiders do a lot of damage.

Well, why was this statute passed? As I said, we were seeing all sorts of conduct, some of which was fairly clever and novel, that made it clear that we needed to address computer crime with some serious new tools. It all started actually in roughly the mid-1980s when an astronomer named Cliff Stole at Berkley found that his grant had run out, and they put him in the computer science lab to solve a small but vexing . . . problem.

Berkley was running two accounting systems to bill users. They were tracking the information in both programs, but there was a 75 cent discrepancy. So they asked Cliff to figure out why . . . . He started investigating, and what he found was that someone had broken into the Berkley system. The person who broke in created an account in one of the accounting programs in the name of "Hunter."

This person did not realize that Berkley was running a second accounting program and never set up a corresponding account. . . . What happened in practice when Hunter signed on was that one program tracked him, and the other did not, resulting in the 75 cent discrepancy. So what did Cliff do? He came to us in the federal government. He said, "Someone has broken into our computer system." And we said, "Well, what's the damage?" And he said, "So far, 75 cents."

So we set up an interagency task force, and we brought in thousands of—no, we said, "Go away, . . . we don't do 75 cent cases, we're the federal government." So Cliff investigated on his own. He found that Hunter was a guy named Markus Hess in Hanover, Germany, part of a group of hackers called the Hanover Hackers. They had been paid by the KGB to steal sensitive, but unclassified, military information from them. Cliff had a bona fide case of KGB espionage, and we told him to go away.

. . . Then in 1988 Robert Morris, a junior at Cornell University, launched the Morris Worm, a little piece of programming code which shut down 6,000 computers around the world in just 24 hours . . . . All of a sudden we realized that our infrastructure was at risk, both the information in Cliff Stole's case, and the hardware itself as in the Morris Worm case.

We are finding, as time goes on, that people get more and more clever about their ideas about how to misuse computers to commit fraud and do other kinds of things. Let me give you a sad example . . . . There was a kid in Washington state who had been convicted in state court of stealing computer equipment and had been sentenced to prison.

From what anyone could speculate and tell, he had a little plan. Here was the plan. He was going to hack into the state court computer and commute his sentence to probation. Now this is a good plan because . . . on the date you are supposed to surrender, the prison has a printout. If you change the information, and your name is not on the printout, everything is okay.

What he did was he hacked through the Boeing Aerospace Corporation and then he hit the district court. The sad part is that he hit the federal district court. He was convicted again. He did not succeed in changing the

right records, but people started thinking about the way we rely on information and the way we deliver government services.

. . . In fact, look what happened to Boeing. No one had any belief that this kid had entered or altered any data in the Boeing system. But because Boeing used this computer system to design the software that flies the planes, they decided they had to check every piece of data on that system, at a cost of $75,000.00.

. . . We have cases like that and cases like Kevin Pollson. Pollson, from California, is kind of interesting. He is a "phone freaker," the class of hackers who attacked the telephone networks. Remember, you talk on the phone all of the time but the phone network is just one big computer network. . . . We have phone freakers who get in the networks and wire tape calls and things like that with alarming frequency.

. . . What Pollson did was he would listen to radio call-in shows. A prize would be offered to the ninth caller after a song . . . . He hacked into Bell, took over the phone switch for the radio station and the ninth call just happened to be his. He won two Porsche automobiles, $30,000 in cash and a fifty-one month prison sentence. The prison sentence was from us.

But the other thing that Pollson did was, because he could access the switches, he could query the switches and ask them for information. What kind of information? Well, for example, he asked the switch who has got a PEN register on their phone. When law enforcement does investigation, we sometimes need to put PEN registers on phones. We get court orders to put a device on your line that tells us the numbers you are dialing.

. . . If you are a drug dealer, we can look at the numbers you dial, get subscriber information and maybe find your supplier. Well, Pollson queried the switch, found out about a PEN register, called up the target and said someone must be interested in you, there's a PEN register on your phone.

. . . When you start thinking about all of the things that people and companies do, the way they handle data and the way the bad guys can figure out ways to manipulate those data and systems, we have a serious problem. I will leave you with one last example because I admire their cleverness, even though it was not appropriate.

There were a couple of travel agents who figured out something kind of interesting. If you book someone on a flight after the plane has left, you do not have to pay for the ticket. Now this may seem obvious to you, but you also still collect all of the frequent flyer miles . . . . They were just booking this guy on this flight after the plane left and then cashing in all the miles. . . .

Who would have thought of doing that before the information age? It would not have been possible. Just stop and think of what would happen if a company like MasterCard or Visa added one penny to one million bills randomly every month. If you got your bill, do you even check it down to the penny? If you did and you saw it was off by a penny, would you do anything about it? But if you do that every month for a million random bills so that no one gets hit more than once every thirty-six months, who would notice?

. . . Computers make all of this possible and people are starting to recognize that and get concerned about it. . . . Because of those things, we now have a new federal computer crime statute.

MR. PERRITT: Thank you. All right, now we will launch into the first hypothetical which will no doubt give us an opportunity to talk about this and some of the other statutes. I think you have it in front of you, but, just to reinforce the facts, I will go through it orally.

A prominent attorney who concentrates his practice on First Amendment issues has created a Web page on the World Wide Web. How many of you have used the Web? Apparently, you have a pretty good sense of what that is. The Web page contains articles and excerpts from recent cases on a variety of First Amendment issues. Potential and existing clients can leave encrypted messages for the attorney at an e-mail address provided at the web page.

. . .

For present purposes, it suffices to say that encryption is a form of encoding messages so that special effort is required to determine either the content of the message or its author. And there are some uses of encryption that also permit the authentication of the sender of the message and, therefore, reduce the risk of forgery.

. . . In the hypothetical, the clients, potential and actual, of this attorney, can leave encrypted messages by sending them to him or her as e-mail. The FBI recently discovered evidence that this attorney is also a pedophile who not only exchanges child pornography through his Web page and e-mail, but also represents individuals charged with trafficking in this material.

An informant has advised the FBI that certain of the articles posted on the Web page are encrypted with pornographic photographs. The FBI also believes that e-mail messages received by the attorney from clients are also encrypted with pornographic photographs. The majority of messages, however, involve unrelated privileged attorney-client communications.

The U.S. Attorneys, at the request of the FBI, have sought judicial permission to monitor the activity of the Web page and to intercept e-mail communications, and we would start by asking Mr. Charney if he thinks the Court can grant the request and what limits, if any, should be imposed on the FBI's activity.

MR. CHARNEY: The answer is yes, the Court can grant the request. The problem . . . in this context, of course, is the issue of co-mingling: the computers are storing more and more data and being used for more and more purposes.

. . . Computers, generally speaking, have in the criminal context three main functions. They are storage devices, in this case for the storing of pornographic pictures. They are communication devices, both for what we call store and forward communication, also known as e-mail, but it can also be real time communications like chat sessions where one person types and the

other person sees the message. And in some cases, the ones we talked about a moment ago, computers can be weapons to attack other systems.

. . . In this context, if we are going to do a wire tap, it is because the computer is being used as a communications tool to transmit pornographic material. The difficulty will be that the same computer that stores or transmits this pornographic material can also store and transmit protected or privileged material.

We run into a lot of these co-mingling cases. We cannot take the position that because this stuff may be co-mingled we cannot do our investigation because that just allows people to immunize themselves by putting on some protected material. . . . Instead, we would ask for a court order and be very cautious about the minimization aspect. We would try to build some sort of Chinese wall so that if a message does not appear to deal with pornography, then we would not look at it.

MR. PERRITT: . . . Before you go on, why do you need a court order?

MR. CHARNEY: We are talking about real time interception of electronic mail, which is electronic communications. It would violate the wire tap statute to intercept it without a court order.[4]

MR. PERRITT: So there is a statutory requirement that you get a court order. Is there also a Fourth Amendment requirement that you get one?

MR. CHARNEY: Yes, because in *Berger v. New York*[5] the Supreme Court said that doing that kind of wire tapping implicates Fourth Amendment issues. But you need to be careful. If we are intercepting e-mail in real time, as it is flying across the copper or fiber, we need a Title 3 . . . . If we want to go into where the e-mail is stored and get the system administrator to give it to us—in this case we probably would not because he is a target . . . —we need a Rule 41[6] for search warrant under § 2703(a).[7]

MR. PERRITT: And do you need that search warrant because the Fourth Amendment requires it or because the statute requires it or both?

MR. CHARNEY: Because the statute requires it . . . . Congress, when it passed the statute, said that the Fourth Amendment might not cover electronic mail, and they wanted it protected in the same way that a first class letter is protected. It may not have constitutional protection. By giving your message to the third party provider, you may have lost your expectation of privacy, so we have protected it by statute.

MR. PERRITT: And what about the Web page? I thought the Web page was open to the public. Why do you need a court order to look at the Web page?

MR. CHARNEY: We do not. The question here was do we need a court order to intercept the e-mail. Most people are of the agreement that a

---

4. *See* 18 U.S.C. § 2703.

5. 388 U.S. 41 (1967).

6. 18 U.S.C. § 2703(a).

7. *See* FED. R. CRIM. P. 41 (providing framework for permissible searches by federal agents).

public web page can be looked at by law enforcement as well as any member of the public. But understand that the Attorney General has guidelines about not looking at things without predication.

For example, if you are walking down the street here, even though you are in a public place, an FBI agent cannot follow you because he or she feels like it. They have to have some sort of predication under internal rules, and the same might apply to web sites.

MR. PERRITT: One other question that I have . . . with the guidelines is it seems like you are talking about several different levels of entitlement to be free of unauthorized searches or surveillance . . . . Is there a remedy for surveillance that would violate the guidelines, for example? And, if so, what is the remedy?

MR. CHARNEY: The guidelines usually do not create substantive rights for defendants. But under the wire tap statute, there are both criminal penalties for illegal wire tapping and civil penalties. An aggrieved party, which is any party whose communication is intercepted or against whom the interception is directed, can sue civilly if that interception is not done pursuant to the statute.

MR. PERRITT: Has there ever been one of those lawsuits?

MR. CHARNEY: The answer is yes, actually . . . . In fact, in the Steve Jackson Games case,[8] in Texas, the plaintiff argued that intercepting e-mail while it was in storage was actually a violation of the wire tap statute.[9] The court, however, correctly disagreed, finding it was governed instead by § 2703, not the wire tap statute.[10]

MR. PERRITT: Did you have a question or a comment?

AUDIENCE: What is the differentiation between the web page and the e-mail?

MR. CHARNEY: E-mails are generally private. You can have public posting. Right now web pages can be public, but you can password protect the Web page and it becomes private space and then the government might need a search warrant, just like entering any private space.

AUDIENCE: So you are calling it Web page and e-mail and it . . . makes no difference.

MR. CHARNEY: It does make a difference in terms of what the technology is. E-mail in this context of this example is private communications between two or sometimes two or more people. Web pages in the context of this, from what I gather, are public web pages that anyone may go visit.

MR. PERRITT: Why not broaden the hypothetical a . . . bit by supposing that as the search warrant is obtained to search the attorney's computer, it turns out that the computer is connected to a local area network at the law firm. And the law firm retains Mr. Miller to protect as much as he can of the

8. Games v. United States Secret Serv., 816 F. Supp. 432 (W.D. Tex. 1993), *off'd*, 36 F.3d 457 (5th Cir. 1994).

9. *Id.* at 441.

10. *Id.* at 442.

law firm's information that's on the local area network .... If you have some comments or arguments with respect to what we have already been saying, by all means start with those and then tell us how you would protect the rest of the local area network.

MR. MILLER: Well by way of background, these guys know a lot more about computers than I do. So they are going really fast .... I want to back up for a minute about the e-mail because I think there is another question that was sort of embedded in your response. My e-mail is on America Online. What I did not appreciate until I started to study for this is that it goes to a storage computer. That stores my e-mail until it is delivered, and the government can access that stored e-mail message.

... In connection with maybe the earlier part of it, explain how you can ... access this message, because I did not appreciate that. I assumed when I hit the little send button, the message is gone and received by the sendee. Well there is sort of an intermediary station where it sits and the government has the ability to access it and even ... AOL has the ability to monitor it, but go ahead. ...

MR. PERRITT: Before you answer, in your answer distinguish, if you will, a genuine intermediate stopping point. Let us say that there is an AOL account through which the message moves. He has an AOL account and let us suppose that the way the AOL system is working today—first of all, this is a kind of heroic assumption that you actually would be able to get into AOL—you get past that and ... you are able to send your message.

... Let us suppose that on this particular day the message comes to rest for a period of time on an AOL computer. That would be called a "mail queue." ... Then ... suppose that it is delivered to the recipient and comes to rest in an E-mail mailbox that is on yet another, non-AOL, computer .... What are the issues in accessing it at different points in its flight?

MR. CHARNEY: ... I think it is important to say, first of all, Greg, that you should not feel bad about feeling that e-mail zips from your machine to the other machine, because if you read the legislative history of the e-mail statute, ... Congress thought that, too.

They actually said that when e-mail is sent, it goes to an intermediate machine until the recipient retrieves it. That is not quite right. When the recipient retrieves the mail, it still stays on the server, which is one of the reasons it is hard to apply these laws to new technologies .... Having said that, here is how it works.

When you get your mail at America Online, America Online is an electronic communication service provider to the public. What that means is that they can look at the mail but they are not allowed to disclose it except under narrowly defined terms and circumstances that are defined by statute.[11]

... If the government wants to access the electronic mail while it is stored waiting for you to retrieve it, you would be wrong to think of this as

11. *See* 18 U.S.C. § 2702.

stored electronically. At this stage it is stored temporarily incidental to transmission. We have interpreted that as follows:

When that mail is at America Online and it is unopened, it is stored there temporarily and incidental to transmission to the recipient. As a result of that, we need a search warrant showing probable cause and we can go to AOL with the search warrant and they will fetch us the message, pursuant to § 2703(a).[12]

Once the mail is opened, though, if you leave it there, it is not stored there temporarily incidental to transmission because it has already been transmitted to the recipient. It is now there for storage purposes, which means we can still get it with a warrant but we can also get it with a subpoena or with a court order under § 2703(d).[13]

All of this, by the way, if I can make a little plug, is actually discussed in the *Federal Guidelines for Searching and Seizing Computers* which we published in July 1994 and can be found on the Web . . . .

AUDIENCE: You are distinguishing the situation where you are actually intercepting an e-mail where you say you need a Title 3 from the situation where it is going through America Online in terms of transmission, and you are saying that you do not need a Title 3 for that, right?

MR. CHARNEY: Yes, and the Fifth Circuit has agreed with us. . . . If you look at *United States v Turk*[14] and also if you compare the wire tap statute, § 2703, which specifically covers things stored with service providers on their way to being transmitted, it is fairly clear § 2703 covers that.

MR. MILLER: Yes, the reason I wanted to raise . . . this distinction is because I know clients feel very comfortable sending you information. You know, you think about it and it is accessible. And it is accessible at the server through a Grand Jury subpoena, which we would not have any notice of . . . . There is some suggestion that the server, that is AOL, would have to give notice, but I think the Department of Justice says they do not have to and I doubt that they would.

MR. CHARNEY: There is a notice provision actually in § 2702(b) where we give notice, but like most notice provisions it is subject to being delayed upon good showing to the court. You usually do not tell targets, "By the way we're investigating you, keep sending the stuff." . . .

AUDIENCE: As a practical matter, how long does AOL hold the material?

MR. CHARNEY: Not very long. I am not going to speak about AOL in particular, because of their volume of stuff and because these companies often change it would not be fair. Some companies, however, store this stuff anywhere from literally twenty-four to forty-eight hours, depending upon volume. That is, if you do not know that we are looking at this person, you can forget it. Or sometimes a small service provider might have back ups for

12. *Id.* § 2703(a).
13. *Id.* § 2703(d).
14. 526 F.2d 654 (5th Cir. 1976).

a week. I do not know of any big service provider that would back up longer than that because of the sheer volume.

MR. PERRITT: All right, let us move on to the law firm local area network question. And, not to lose some of these issues about, where the e-mail has come to rest. . . . suppose that some of the e-mail . . . coming to this attorney has originated from private networks that are connected, and that have electronic access to this law firm through the Internet.

In other words, there is no commercial intermediary of the AOL or the CompuServe sort involved. We have, at least for starters, . . . a private computer . . . managing the sender's e-mail, and it comes directly through the Internet to the private computer and local area network that manages the e-mail on the receiving end.

MR. MILLER: . . . At this stage of the hypothetical, the FBI is at the law firm and conducting the typical FBI search. They are seizing everything and planning to sort it out when they get back to the FBI office. And, in the process, they are trying to advise the law firm on the significance of this search. . . . I can tell you these are now becoming real issues in terms of how they search.

The computer is part of a network. So, first . . . we look at the search warrant. The search warrant, because of some fine work by Scott if they have read the directions given to assist the U.S. Attorneys, they have told them exactly what they asked for in the search warrant. So they have asked for the hardware: the computer, . . . the keyboard, the printer, the modem, everything that connects it to it . . . .

If they have done their homework, they realize that it's part of a network and now they may have said, . . . "We also want to . . . follow the chain." And in this law firm they have the network server that may have data on it.

MR. PERRITT: . . . Indeed, it is that computer that most likely has the e-mail mailboxes on it.

MR. MILLER: Exactly. So now we are talking not just about the computer . . . sitting on the attorney's desk, because they have taken that. That one is gone, alright. But now we are talking about a network server that might not only have that attorney's material, but it may have every other attorney's material on that computer.

And the FBI now is unplugging your server and saying they are going to take it back and . . . sort through all of this material and when they finish they will let you go. Well, if you have a network in your law firm, you are essentially shut down. You cannot retrieve any materials. You cannot print anything—letters, correspondence. Plus, a tremendous amount of privileged material is on that server computer.

. . . It is interesting that . . . this situation, and I think it was even suggested in Scott's *Guidelines for Prosecutors*, . . . may be an appropriate example of where you go get a special master. You petition the Court and say, look, this is really a serious issue. There are privilege issues involved here.

We cannot simply let the FBI do as they may do in other searches, look through all the data and say we promise we won't look.

You as an attorney have to protect this confidence. So even though we might hate this lawyer, we cannot consent to this search. We have to make every effort to protect the privilege . . . .

MR. PERRITT: What is the procedural framework for your seeking that?

MR. MILLER: . . . There is a case where it was approved. I can give you that cite here in a moment.

MR. CHARNEY: Okay, while he looks for that cite, it is also interesting to distinguish this kind of case, pornography, for example, from other kinds of white collar cases. If all the government needs is information from the system, like records, you can go in and make a copy of the records and go away with the copy and leave the machines intact.

The interesting thing is that you need to focus on whether or not you are interested in the computers and the hardware or just the information contained therein. One of the things that makes it difficult in a pornography case, an obscenity case, or a child obscenity case is that the computers used to transmit it are tools of the offense and also forfeitable under federal law.

. . . Because of that, if you went in, for example, in a kiddie porn case and just copied the data, you run into two problems. One is that you have left the machines and tools there. And, two, you have left the original pictures there . . . . That situation is somewhat different from one where you want records and do not care . . . if copies of those records are left at the law firm. And you have to keep thinking about that distinction because it becomes critically important in deciding whether we are actually going to seize boxes or do on site searches.

MR. PERRITT: . . . Why does it matter if you leave the original pictures there?

MR. CHARNEY: Well, they may keep distributing them . . . . It would be hard to explain to the public why we found these child pornography pictures and allowed the defendant to keep them.

MR. MILLER: The case that I was referring to is a Ninth Circuit case *DiMasa v. Nunez*,[15] which authorizes the use of a special master. Another approach, . . . if you do not have a special master, is . . . to have the FBI sit down with your computer person and say, look, we will cooperate with the search but let us work with your computer expert so that we can be quite discreet in how . . . we search this information.

. . . In many cases they may agree to go along with that as long as there is some guarantee that if they want to come back at a later date to review the information, they have the ability to do so . . . . We have negotiated situations with the FBI and they usually bring computer experts to these searches who are very knowledgeable on how to retrieve data or . . . bypass systems.

15. 747 F.2d 1283 (9th Cir. 1984).

Also, there are passwords and other things that might . . . protect your system and you may be willing to share those. It makes their lives a lot easier if there is some cooperation . . . . In this case it might be in your interest to cooperate, have your computer specialist work with the FBI to retrieve only the information within the scope of the subpoena.

MR. PERRITT: But assume you get a special master, where is the LAN server going to stay? Is it going to stay plugged into the LAN or is all this going to happen down at the field office?

MR. MILLER: Well, I think you would try to convince the master to keep it there, but you would have to give some protections. The big concern you have with this system is that it is accessible . . . . Presumably the bad attorney, if he wants to, . . . might be able to access that computer and delete information. So you are going to have to . . . satisfy the special master that you can protect the information. If not, the server is gone. They would take the server.

MR. CHARNEY: I would point out, in the case I told you about the two travel agents who were booking this John Doe character, the original affidavit for the search warrant was to seize the LAN of the travel agency. And when we discussed it with the FBI we learned that there were actually two targets in the travel agency of twelve people. So we decided not to do that.

We went in, talked to the owner of the travel agency who was actually very annoyed that his . . . agency was being used in this way, and just copied the data on site with his help. We took two machines that those two people were using, and we left the rest of the network and the server intact.

. . . When you go into a situation where the entire organization is not corrupt, you can work with someone who is often a victim . . . . Most law firms, as well as private companies, do not want their networks being used for the distribution of child pornography, or even any kind of pornography, not even obscenity, because employers are starting to get sued for creating a hostile work environment when employees have that kind of material.

. . . In that environment the employer is often very willing to work with you to help you get the evidence you need in a way that . . . does not disrupt their business.

AUDIENCE: With respect to doing that in reference to the AOL scenario, what obligation, if any, is there on behalf of AOL to be accountable if they actually see the target letter? . . . . Actually they are not going to disclose the target, but is there any obligation incumbent upon them? . . .

MR. CHARNEY: No, the disclosure requirements are on the government, not on the service provider . . . . It depends on what we are doing and at what juncture . . . . For example, we have had cases where the target is actually arrested and we believe that there is evidence in his mailbox . . . . Then you do not care if he knows. You tell him, "Look, we are going into your mailbox. We are getting a court order." But if you have an ongoing investigation that is still covert, then, of course, you seek a delay.

MR. PERRITT: Is AOL prohibited from informing the target that there has been a request?

MR. CHARNEY: I do not know that the statute actually prohibits it. Off the top of my head I cannot tell you. We never have had a case where they have disclosed, though.

AUDIENCE: You had mentioned that AOL can look at the message while it is being stored. I think you referenced some disclosure or affirmative disclosure obligations?

MR. CHARNEY: Not affirmative. Under § 2702 a service provider to the public may disclose the contents of a communication in electronic storage on its servers if they have the consent of a sender, recipient or addressee or intended addressee.[16] If it is necessary to protect their service from abuse and protect the rights of the provider, if they get the contents inadvertently and it appears to pertain to the commission of a crime, then they can disclose the information to law enforcement.

And I think there are one or two more but they are all built on the consent of senders, recipients, or addressees. Private providers can look and can tell . . . . There is no prohibition on private providers.

MR. PERRITT: . . . Suppose that the most interesting stuff looks like it might be the encrypted stuff, can you compel the attorney or anyone to provide the key to unlock the encrypted messages or files?

MR. CHARNEY: You can probably subpoena the key if it is a stored document. Because key lengths and encryption keys are very long, they are often stored electronically. So they can be searched for or subpoenaed like anything else. But if the key is a memorized key, then you would have serious Fifth Amendment questions. If you said to someone, tell us your key, they could plead the Fifth.

MR. MILLER: I think at this part of the hypothetical, Scott informed me, . . . you mentioned a very technical term for encrypting photographs into text. I will let him explain that to you because that is what is intended by this hypothetical: it looks like a regular memo but, in fact, it has pornographic pictures in it.

MR. CHARNEY: There is a form of encryption called stegonography . . . . Basically what stegonography does is, . . . assume I have a text file. On the screen it looks like a text file but on the hard drive, on the plotter it is just a series of zeroes and ones. It is all bits. Then I take a pornographic picture or a copyrighted software or evidence, a confession, or whatever, and that is a text file or a graphic picture file and that's a certain number of bits.

There are programs that will take the bits from the pornographic picture and scatter them among the text file . . . . Unless you know the codes that tell the scattering program to go retrieve all the bits in the places that they have been embedded in the other file, you will not find them. See, part of the problem with encryption and stegonography is that you can talk about doing

16. *See* 18 U.S.C. § 2702.

searches on site, but if you are going to run into cryptography like that it is fairly sophisticated, you are not going to break that on site. You will have to take it to a lab.

That complicates the issues for law enforcement. As much as we are doing more searches on site in computer environments than ever before because we can do mirror imaging of bits, more and more people are finding out how to hide bits in systems. And if you think you are dealing with someone very technically sophisticated, you need to secure that evidence and put it in a laboratory environment and use forensic processes that the courts will recognize as valid. So it gets harder and harder to do things on site.

MR. MILLER: . . . That is why the issue I think will come up where a criminal defendant or punitive defendant or even a third party is compelled to provide the key to the encryption that occurs on this material, this information. So I think it is ripe for a challenge at some point in the future. There is no case now that I am aware of where someone was compelled, but if you think about it, they compel you to produce handwriting exemplars, they can compel you to produce photographs, they can even compel you to surrender keys to safety deposit boxes and things of that nature. So it does not seem far off that they will be pushing in this area to compel someone to provide the code to unlock an encrypted information on a computer.

MR. PERRITT: Just to make sure I understand that, could we distinguish four different circumstances? One is where a third party has the key and it's stored. The second is where the criminal defendant has the key and it's stored. The third is where the criminal defendant knows the key but it's not represented except in his head. And the fourth is where there is a key escrow arrangement, explicitly denominated. What are the issues in compelling access to each one of those four?

MR. CHARNEY: Well certainly if the key is stored, whether it be by a target or a third party, it could be subpoenaed or searched for. The choice between a subpoena and the search warrant would depend heavily, of course, on the role of that third party. If they are just independent witnesses, you can give them a subpoena and they will honor it. Defendants who are targets are not very good always at turning over things pursuant to a subpoena, so you might go in and search for it.

MR. PERRITT: And there are no Fifth Amendment issues when you do that?

MR. CHARNEY: Not if it's a pre-existing stored item because it wasn't created at the compulsion of the Government. On the other hand, with the key escrow agent, which is basically a third party who holds keys, there's legislation on the Hill now that it will develop what we call a key management infrastructure.

And that legislation will also provide for when a keyholder needs to turnover a key and what level of proof and what kind of documents the Government has to bring to get that key. If the key is in the person's head, well then you've got a Fifth Amendment problem. Of course, you could call a person to the grand jury and immunize him to get the key.

There will be, of course, acts of production, privilege issues, immunity issues. If it's a low level player, like a bookkeeper, and you're willing to immunize him to get the higher level, well then it would be no different than other kinds of testimony . . . .

AUDIENCE: Do the sender and the receiver have to have a key?

MR. CHARNEY: The answer is no. You have to distinguish between private key cryptography and public key cryptography. In private key cryptography the sender and recipient have the same key. The problem with private key cryptography is we need some message of exchanging the key. We need to manage if very carefully. If Hank and I want to have a private key session, how do I get him the key?

If I send it with the message, anyone who intercepts the message intercepts the key. So that doesn't work. So I have to call him up and say, I'm sending you a file, the magic word is. They're tapping my phone and they get the magic word. More importantly, I have to know Hank to make that call. How do I send messages to people I don't know? So Whitfield Diffy and Martin Helman back in roughly '76 developed public key cryptography and here's how it works.

You have a public key and a private key. That is each key — and the keys are generated by using two very, very large prime numbers. It works on the theory that multiplication is easy but division is hard. If I give you two very long numbers, you could on a piece of paper multiply it out. You'd have a lot of rows and columns, but you could do it.

But if I gave you a really huge prime number and said to you, what two prime numbers, when multiplied, give you this, knock yourself out, okay? Here's how public key works. We generate these keys, I have a public key and a private key. I post my public key. Everyone had access to my public key. You encrypt the message with my public key. My public key will not be crypted. It's a one way function.

You need the private key to decrypt it. I keep my private key private. So anyone can look up my key, send me a message and I can decrypt it but no one else can. So I get a message from you and say, well I want to send him back a private message. So I look up your public key, I encrypt my message in your public key, send it back and use your private key.

The beauty of the system, of course, is we don't have to know each other. Moreover you can reverse it. I can post something with my private key and everyone can use my public key to decrypt it. Why would that be valuable? Well, if it's an article on a Web site, you'd know I really wrote it because my public key worked against it. Now public keys are prime numbers. They're very, very long. Because they're so long, it takes a long time to do encryption and decryption.

So the public, private key pair is not really used to encrypt and decrypt messages. What happens is we choose a session key for the one message which is much shorter, still very robust, but shorter. We encrypt the session key with the public key and the message with the session key. So essentially

what happens is you have a message using the public key encryption in order to get you the private key.

. . . So we take the message, we encrypt it with something workable, and we take the workable thing and encrypt it with something very big. So we exchanged the private key for the session with public key cryptography . . . .

AUDIENCE: The issue of the search warrant, how does one go about narrowing it so that in this instance, number one, the attorney-client privilege is respected, number two, who is making the decision on whether it's privileged material, and, finally, how do you narrow the scope of the search so that when the agents pull up and back the truck up to the door, they don't knock the firm out of existence until you can get the specialist? How do you design a search warrant to handle those issues?

MR. CHARNEY: It's actually fairly difficult, as you might imagine . . . . Remember, search warrants have to be issued on probable cause. And not unlike other situations, what you need is probable cause that a particular individual is using the e-mail system to commit a certain offense. And it's person-specific.

So on a bulletin board service or on a web site with a lot of e-mail, if you believe one person there is sending obscene material with other people but you don't know who the others are, you can only get a warrant to search this person's e-mail, not unlike wire tapping where you say this phone is being used.

Here's the problem. We can narrow it down to that person and then if we open up a message and this person is transmitting obscene stuff to and from Hank, we can go back to the Court and say now we have PC on Hank's mail. The problem is within the mail there will be mail that's related to the crime and mail that isn't.

In the wire tapping situation, what we do is we listen to the beginning of the call. If it's not related, we stop listening. It's no different when you review documents. If you're looking, for example, for child porn pictures, you can look at the headers of files for GIF files and other formats that are pictures and ignore text files. In fact, computer technology allows us to enhance privacy protection. We are building tools that automate the search process.

What happens is a program looks at the data and says, this is a .GIF file, which means picture file, this is a WordPerfect document, right? And if you do that automated, then what the program does is it kicks out to you and says here are the pictures, this stuff is not pictures. You don't even have to look.

So what we're trying to do is use the technology to do the searching for us in part because we're just getting too much data, and also filter out the criminal stuff and protect the private stuff. The difficulty with this is if the person is using the e-mail system and the web not just for pictures but they're communicating and talking about doing things with obscene pictures and kidnaping kids and doing this and that, it's very hard.

MR. PERRITT: But even before you get to that special problem in the automated search, the important part of the search warrant is now in the

computer code for the program that's going to search this and omit that. The magistrate doesn't write the computer program.

MR. CHARNEY: No, and in fact, . . . those of you who use word processing programs, for example, like WordPerfect or Word, know that you can search for a string, a text string. So if you know that your bad guy uses the word "surfboard" whenever he means cocaine, you can search through a whole directory of files looking for the word "surfboard."

And you can also say, if I don't get a hit on that word, this document is not related to cocaine-trafficking. The problem is that only works if you have enough facts that you can build a search criteria that's meaningful and doesn't miss most of the evidence.

MR. PERRITT: How does the magistrate satisfy herself that your program does what you say it does?

MR. CHARNEY: What we have done, even with commercial off the shelf programs, like Norton Utilities, is we've done scientific tests on the program. For example, if we're going to copy data on site, invariably the defense will claim our copy is no good. So what we do is we take the program, like a Norton Utilities, and we copy a lot of files and then we compare the files with different tools to prove that when it says copying it really is copying. And then you call up the vendor. And if need be, you call the programer to testify how his program works.

MR. MILLER: What's very interesting about this whole process though is that Scott is sitting down with the magistrate and they're explaining all the special techniques that they have but, you know, nobody from the defense is there to challenge the effectiveness of this program and to respond to your question while they have the ability to search through this information.

Generally they do it back at FBI headquarters where they have time to be careful because there's other things that people do to computers. I mean, they set traps and bombs and other things that are designed when someone that has not authorized the search begins the search. It destroys the data. So they have to be very careful when they conduct the searches and the best place to do that is back at the FBI laboratory. So it's gone. Okay, your computer is gone . . . .

MR. CHARNEY: In fact, when we did the Masters of Deception case, a hacking case in New York, we were doing a wire and data tap. It was our first data tape over the telephone network. And the bad guys had been talking on the phone about how gamblers had flash paper. That when you put a match near the flash paper, everything went up. And gamblers had this wonderful paper so if the police knocked on the door, everything would be destroyed.

And they said, you know, let's wire our computers the same way, that if there's a knock on the door we can just hit a set of keys and everything will start deleting itself and overriding. And based on those conversations, we got a no-knock warrant . . . .

AUDIENCE: Not to minimize the complexity of what you're speaking about, but it strikes me that it's age old problems, just in a new medium. I mean, if you're searching for documents at a business, you have all the same old questions as do you take the originals or do you make copies? And if you make copies, do you Bates stamp them to prove that they're the copies? Because in a business when you take the copies, and you go through the pieces of paper that may be attorney-client privilege and how specific do you have to be to go through all of the records or just some of the records.

So, again, I mean I sort of dropped back to the fact that from a legal point of view, the issues are pretty much the same, you just have to have somebody nearby you who understands the computers and assists you to translate the same old issues into a new medium.

MR. CHARNEY: That is true as an issue but not in execution, and here's why. If I go into an office and I've got five file cabinets with five drawers, I've got twenty-five drawers . . . . And I'm in a situation where I don't want to disrupt this business, if I send in twenty-five agents and give them each one drawer, we'll be done in an hour.

But if you've got a hard drive with 2.3 gigabytes, I can send in twenty-five agents and twenty-four of them will watch the other guy access the computer because all of this stuff is co-mingled together. You're right, the issues are the same, how do you protect privileges, do you make copies or take originals, absolutely right. But the execution becomes very problematic because of the technology. You cannot encrypt paper documents. You can encrypt bits by scrambling them around.

MR. PERRITT: Let's move onto the second hypothetical and then if we want to return to some of these issues, we can do so at the end.

The general counsel of a major international corporation has been advised that several employees are complaining about racist and anti-semitic information that's been appearing on the company's intranet. (An intranet is exactly the same technology and software that's used for the Internet but certain computers that provide linkages between the internal computer system and the external Internet have been programmed so that some information stays inside. That's all an intranet is.)

After conducting a brief investigation, the general counsel learns that a group of employees have formed an organization called "Real Americans." Members of the organization prominently display a screen saver at their desk figuring an upside down flag. They also apparently exchange information and articles that may be considered racist and anti-semitic via the company's intranet.

The general counsel now has authorized an internal corporate investigation which includes the interception of communications on the intranet.

What are the legal implications of the general counsel's action? By legal implications, I would like to start—and perhaps finish—with crimes rather than civil liability.

MR. CHARNEY: Well I was actually going to say that if I got this kind of call, it would be very easy to handle because we don't give legal advice to private parties and I would just refer them to Greg.

MR. MILLER: And I would tell the general counsel that the employees enjoy no significant rights concerning information contained on a company's intranet. So even though this hypothetical strikes you as some form of surveillance of electronic information, as a practical matter there really isn't an issue here. They have the ability to access this information.

And while I was looking at this issue, I found a statistic that I thought was a little interesting in terms of how frequent this might be, because many of us function in environments where we deal with intranets. And it says, a 1993 survey in MAC WORLD magazine reported that 22% of companies engage in searches of employees' computer files, voice mail, e-mail and other network communications. In companies with one thousand or more employees, the figure rose to 30%.

Based on survey results, the magazine estimates that twenty million Americans may be subject to computer monitoring on the job. It would appear that while the legality of monitoring is still unclear, companies are taking advantage of the uncertainty and only 18% of . . . companies has written policies regarding electronic privacy.

MR. PERRITT: Why isn't this a misdemeanor under amended 18 U.S.C. § 1030?

MR. CHARNEY: Because you have to access a computer system without authority and it's very doubtful in most cases that you can claim that the entity that owns the machines and administers the machines can actually exceed their own authority in accessing the machines.

MR. PERRITT: Suppose the entity that owns the machines has issued a formal policy that says your e-mail boxes are private and we don't access them?

MR. CHARNEY: The problem is there's actually been a case like that where an employee was told the mail wouldn't be read. It was . . ., I think, here in Philadelphia and the Court held that this employee did not have a privacy right in the e-mail. And the cases where employees have sued, like *Shoars v. Epson*[17] and stuff, they have routinely lost on this issue. . . .

AUDIENCE: In working in criminology again, could there be, you know, in a business place you can search or maybe get authorization to search everything except maybe the drawers of an employee's desk or something which may be considered private, it seems to me there's got to be somewhere within an intranet system where an employee could establish an expectation of privacy, whether it be by way of password or the nature of the information. I mean, I find it hard to believe that it would be a blanket permission to search intranets, that there wouldn't be some privacy somewhere.

17. Shoars v. Epson Am., Inc., No. S0H0065, 1994 Col. LEXIS 3670 (Col. 1994).

MR. CHARNEY: Well stop and think about this. Suppose an employer went into an employee's office and the desk is there, they want to look in the desk which is owned by the company and the person also has a briefcase, okay? In *O'Connor v. Ortega*,[18] the Supreme Court said with regard to government searches it's clear that individuals, even government workers, can have an expectation of privacy in government space.[19]

And in support of this, they actually talked about things like briefcases or luggage before a long weekend. One of the issues that comes up which is a little harder to deal with is when an employer in the government context wants to look at an employer's machine, right, and you say we want to look at the machine, and we want to look at the floppy diskettes.

And so they go in the office and there's the machine which is owned by the government for government work and then there are five diskettes. And the first one says, you know, *United States v. Jones* and then . . . the fourth diskette says home. What does that mean?

Does that mean this employee uses this disk owned by the government to take work home or does this mean this is a disk that they brought in from home that is personal property?

MR. PERRITT: It seems to me that there are lots of employment law privacy cases in the purely civil context that would be supportive of the notion that, if there is a climate created where the mailboxes are private and the employer has acted consistently with the mailboxes being private, there would be a pretty good common law invasion of privacy claim if the employer accessed the employee mailboxes.

And that's why counsel regularly advise employers to make it clear that they should promulgate some sort of policy and make it clear in the policy that there are at least some circumstances under which the employer reserves the privilege of accessing the e-mail boxes.

Now there is still, (and I realize I'm doing what I encouraged the others not to do, I'm talking about civil liability instead of crimes,) the possibility that if the employer announces its intention to police the employee e-mail boxes, then it opens itself up to greater levels of liability if some third party objects to something that's in the e-mail.

Let's say that an employee is trafficking in infringing material—copyright infringing material. Well, if the employer has no knowledge—and no practicable way to gain knowledge—of the employee's activity because it's all being done by e-mail and it's in the e-mail boxes that the employer doesn't access, then the likelihood of the employer confronting liability is low.

But if the employer has announced to the workforce and to the world that it regularly checks the e-mail boxes for bad stuff, then the likelihood that it should have known of the infringing character or other harmful character of the information is much higher.

---

18. 480 U.S. 709 (1987).

19. *Id.* at 725.

MR. CHARNEY: You should also know that in a recent survey by War Room Research, about 66% of the respondents, which were mostly large companies, said they had banners on their computer systems advising employees that they reserved the right to monitor such systems.

MR. PERRITT: Suppose the general counsel comes to the FBI and urges that these "real Americans" be prosecuted, is there any possibility of prosecuting them under federal law?

MR. CHARNEY: Well, you have a separate problem in the context of this hypothetical which is this is protected speech so there's no crime, so we tell them to go away.

AUDIENCE: What is the material that's contained on the computer system, the material that violates the employer's policy about what material can be placed on the computer system? Can you state the position that the employee has, therefore, exceeded authorization to the computer?

MR. CHARNEY: You have to exceed authorization and obtain information you're not supposed to have. I don't know that in this context they're obtaining any information. I'm not sure how you would show that this is an impairment to the integrity or availability of the system. . . .

MR. PERRITT: But if he's running a pornography ring, it well might bog down the network so much that other people couldn't use it, which is not too different from what Robert Morris did on with the worm on the Internet.

MR. CHARNEY: . . . We have cases like this with service providers now. For example, someone will send so many e-mails. One thing computers can do is generate a lot of packets, okay, which are basically messages. Computers talk in packets. Each message is broken up into little pieces and routed to a destination. There are things that are affectionately known as "packet cannons," which will shoot so many packets at a system they will shut it down.

If a person is doing that, for example, because they are mad at the company and want to put them out of business, that's a denial of service attack, then it becomes a criminal matter. But you have to intend that. So if, for example, these people said let's send out a lot of packets because we want everyone to know our message, and it shuts down the system, it's doubtful you can show they intended to shut down the system.

Just the opposite, they wanted the system to stay up and running because they were trying to deliver a message. So you probably look at the intent element and say no, we don't have a crime here.

MR. PERRITT: Suppose the employer has arranged a "firewall." (That's a border or gateway computer that can isolate various parts of the internal system.) Suppose the employer has arranged the firewall to exclude traffic, to exclude .GIF files? That would not be easy to do but it would be possible. And our internal—our misbehaving—employee, without authorization, alters the firewall so the .GIF messages can get through and he can continue to run his pornography ring. Is that a crime?

MR. CHARNEY: If he has now impaired the integrity of the system and the cost of that was over $5,000, then you might have a 1030(a)(5)(a), but the damage would have to be significant enough and you might have difficulty in this case showing that kind of damage since all he did was probably tweak the filter and it would take somebody just a couple of minutes to tweak it back, it probably wouldn't meet a monetary threshold.

MR. MILLER: If we took the hypothetical of protected speech, I think that's where you were going, and I'm the employer and I say, "We're now going to consent to your access to this information," are you going to take my consent? Are you going to accept it? Is that going to be good enough to justify accessing the information on the intranet?

MR. CHARNEY: Right, it would be a third party consent . . . if you have real or apparent authority over the area searched, we could take that consent. But if you were doing real time monitoring as a service provider, not an internal company, and we came to you, you would then become our agent and we'd go and get a court paper.

MR. PERRITT: . . . Why was it necessary to amend 1030? You touched on that a little bit, but tell us more completely why those extensive amendments to 1030 were made.

MR. CHARNEY: If you looked at the confidentiality provision, for example, of 1030(a)(2), it protects financial records possessed by financial institutions but no other kinds of data. And we've had people hack into hospitals to get medical data and other kinds of data that should be protected. We also had a funny thing with 1030(a)(3). 1030(a)(3) is a trespass provision. It makes it a crime to trespass in a federal government computer. It's a misdemeanor.

And Congress drafted the language in a very particular way. They said anyone without authority to access any computer of a department or agency who accesses such a computer is guilty of a misdemeanor. And so when I got involved in computer crime, I said, "What is this, any department — computer of a department or agency? Why didn't they just say a government computer?"

It turns out what they meant was this. I'm in the Justice Department. I'm authorized to access my machine. So I am authorized to access a computer of the Justice Department. If I hack into the FBI, because I'm authorized to access a Justice Department computer, it is not a crime. What Congress says is if you're working internally, be disciplined. Maybe lose your job, but it's not a crime.

But if I were to go into the Treasury Department where I'm not an employee and don't have authority to access a computer of the Treasury Department, then I'm an outside hack or it's a crime. So when we proposed S-982, the National Information Infrastructure Protection Act,[20] which was written by our section, we left that provision intact because it had worked fine, we didn't have a problem.

---

20. 18 U.S.C. § 1030 (1996).

So I'm down at Maxwell Airforce Base and I'm talking about our proposed amendments at that time to the statute and how we left 1030(A)(3) alone. So this student in the back raises his hand, he has a question. I said, "What?" He says, "Does the Justice Department have a web site?" And I go, "Yeah." And he says, "So everyone on the planet is authorized to access the Justice Department computer." I guess this has been repealed.

So we went back to the Hill with a little tweak and now it's a crime if you have no authority to access a non-public computer of a department or agency, okay? And then we thought about that. I mean, we ultimately went that way and that's what Congress passed, but what's non-public? What happens if someone accesses your public computer, a web site, and then hacks it? Not that that can ever happen, even though we got hacked just that way, okay?

So we started looking at public portions and non-public portions, and we just said it gets too confusing. One of the things criminal statutes have to do is give fair and clear notice. So if you start talking about public portions and non-public portions, people might go and hit links and go somewhere they're not supposed to go and it gets really ugly really fast, so we opted for a very clear rule, even if it's a little under-inclusive.

MR. MILLER: One thing that I thought about and would be interested in your point of view on is what about notebooks? Everybody now has notebooks. I mean, when does a notebook no longer become a computer and become a diary or become something that there might be some greater expectation of privacy, some greater requirements in terms of Government access?

MR. CHARNEY: Notebooks, of course, are treated like other forms of personal property. It is problematic because people do target notebooks at airports. They do that when you put your laptop through the X-ray machine, somebody will block your path through the machine and steal your notebook on the other side. They do that because they can get information about your company or agency.

And if there's no interesting data on it, they still get a $4,000.00 laptop. So what's the downside of this? We generally treat it like any kind of property. The interesting thing, of course, is how you define "computer" for these laws. Most international experts believe you cannot define the term "computer."

But, in fact, Congress has defined it. It is any electromagnetic, optical, electronic or other device capable of doing storage, processing or other functions. And it's kind of interesting when you look at that definition and you think about the history of the microprocessor. Because what happened was in the early '80s the XT chip came out and then the 286 came out. It was a completely different architecture.

And everyone said, "Oh, this is going to be great. We're going to write all of this new software, it's going to be terrific." And before the software came out, the 386 came out and the 286 became obsolete. So what happened

to all of those 286 chips? They made millions of them. They put them in electronic devices, microwaves, cars, cellular phones.

Okay, now in my office we have a microwave. So you go into my office and you use the microwave, you put in the time, the temperature, it stores that information. You hit start, it processes. It's also illegal, of course, to access a Government computer without authority.

MR. PERRITT: Let me broaden the inquiry just a little bit in the following way. We've been talking about computer crimes in terms of how the law punishes people that commit them. Another way to respond to the potential for computer crimes is to reduce the risk by the way you use the technology. I spend a lot more time talking to people about using the Web for electronic publishing and for improving access to information than I do talking about computer crimes.

But as I talk to legal institutions—law firms, courts, legislatures—about how they can make effective use of this new implementation of the technology to reduce their costs and improve the ease with which people can get to information that they consider to be public and that they desire that their publics have access to, many of them, a significant number of them (fewer over time), say, "We think that's a good idea and we think that's a good use of the technology and we'd like to have a Web page that has all of our opinions accessible through it, but we're afraid to do that because we went to a speech not long ago that Scott Charney gave. He was telling all these stories about people that had gotten into the telephone switches and turned things around and gotten into the records of convictions and changed the incarceration determination to a probation determination, and we're afraid that if we open up our computer systems to the public through the World Wide Web that there will be an unacceptable risk of this new kind of computer crime."

My response always is that there are ways to manage the risk of intrusion so that you reduce it to acceptable levels. That . . . ought not to stop any institution that I know of—any institution in the United States—from making use of the Web to enhance public access to the materials that it intends to be public.

For example, if you are very concerned about the potential of intrusion into sensitive data, what you do is you set up your Web server and you don't have any electronic connection between the Web server and the rest of your computer system. That's the way the Supreme Court of the United States has been disseminating its opinions in electronic form for ten years, long before people were doing it on the Web.

More often, it is an acceptable level of risk if you connect your Web computer to your local area network with your other resources on it, but you have very carefully programmed firewalls at various points in the system so that you isolate the packets from the outside from the sensitive material on the inside. That is a well understood process.

There are ample numbers of professionals in almost any metropolitan area that know how to set up firewalls appropriately. And, therefore, there is a range of precautions, technical precautions that should make it possible for

any institution to publish electronically through the Web. But I wonder what your reaction is to that position?

MR. CHARNEY: Well that's absolutely right. I mean, computer security is risk management. That's what it is. Let me give you an example. Many courts have bulletin board services where you can dial in and see docket information and all that stuff for publicly filed stuff. So how did the Eighth Circuit do it?

Well the Eighth Circuit had this LAN . . . where their judges could do their work and there were unpublished opinions and they could e-mail each other and they decided to set up a public bulletin board service. So they took one of the machines on that LAN and partitioned the hard drive into two halves and put the public stuff on one half. It took a thirteen year-old roughly twenty minutes to jump the partition so they could access unpublished opinions, okay? That's bad planning.

On the other hand, if they wanted to do that, and so they took a machine and dedicated it to this purpose and put a modem on it and plugged it into the wall and had no other information on this machine, that would be fine. The problem with that approach, of course, is as new opinions are published, you would love to just be able to e-mail that opinion to this machine, okay, you can still do that.

You have to sign onto that machine with high level privileges that allow you to alter information, okay? So it can be done but it's risk management. The FBI spent a lot of time, before we put the ten most wanted pictures on the Net, we spent a lot of time figuring out how to do it right. The last thing you want is some hacker to get in and remove "Wanted Number Nine" and replace it with a picture of his next-door neighbor because that's not pretty.

MR. MILLER: One other thing that I thought to go back to the first hypothetical for a minute and just turn it into practical terms, I would say that there are probably no search warrants now being issued by the Department of Justice that don't somehow address computer information. I mean just about any place they search, in homes and things of that nature, they're going to have a request for computer data on that.

. . . That's probably the most significant thing you're going to see in your practices if you represent hospitals, physician groups, I mean almost everything they do is on their computers. Their computers are a critical part of their practice and the government is going to want to know information that's contained on that. And so as reluctant as I have been to join the computer age, if you're going to practice, you've got to do it.

I mean, these are issues that are real, they're out there. You may not have addressed them yet. The Department of Justice, quite honestly, is ahead of most of us private practitioners in understanding computer-related issues, what you may be advising clients in the criminal context and without a full understanding of some of these computer issues, you may miss some very big issues.

AUDIENCE: . . . Is there material that is available? You know, you mentioned —

MR. CHARNEY: The *Federal Guidelines for Searching and Seizing Computers* is available at the web at www.usdoj.gov/criminal, because we're in the criminal division, /cybercrime. Additionally, it's been . . . published in full by the Criminal Law Reporter, text number five, December 21st, 1994, Volume 56, number XII at 56 Criminal Law 2023 . . . .

MR. MILLER: I've got to tell you that this is a very, very good place to start in terms of these issues. If you'll see here, the author of these guidelines is Scott. But in there they cite most of the leading cases on these issues.

MR. CHARNEY: Many people worked on this. It was done by an inter-agency group because we felt that federal agents, both in different agencies and even agents within the same agency were doing these things differently and there had to be some better way to harmonize this.

The other thing is that the Criminal Law Reporter has just published our analysis of the new 18 U.S.C. 1030 bill, the Computer Fraudulent Abuse Act. Because we wrote the bill, we wrote a proposed legislative history. And although it was not adopted by Congress, we have published the document that basically has all of our reasoning for what we did in each section.

. . .

MR. MILLER: And in it, it has a lot of the case law discussion of privacy issues, consent. It talks about how they come up with their descriptions of data for search warrant. And I always love it when the Government publishes guidelines because even though they don't create any substantive rights, you can always say you didn't follow your own guidelines in drafting your search warrant and you may have some reason. And this is where I found the case that proposed the use of a special master. So I think it's hard for the Government now to complain about that as an option in the appropriate case.

MR. PERRITT: I'd like to make a comment about the observations earlier that there's nothing new here. I agree with that in the fundamental sense. There's nothing about this technology that changes legal doctrine or that changes the balances that society and the political institutions have struck and expressed in law, whether common law doctrine or statutory law.

In that sense the new technologies are not revolutionary. They might seem to be not even interesting because they are like the file cabinets and the written documents. That does not mean, in my view, that a lawyer need know nothing about the technology and simply can rely on technologists. It does matter quite a lot whether a third party has the information at some point.

And if you don't have any idea at all about the architecture of the electronic communication system, then you aren't going to know that there's maybe a third party involved. Similarly if you don't have any inkling of how e-mail technology works, you may miss some very important factual distinctions about where it comes to rest and who has it and so on.

Now in acquiring that level of knowledge about the technology, there's some good news. You don't need to know anything at all about computer

programming. You don't need to know the first thing about how a microprocessor chip works. All you need to know is how the resources that make up a computer network are organized.

And that doesn't require any more scientific knowledge than is required to understand how a bus company is organized or how an automobile manufacturing operation is organized. So the level of knowledge that's required about technology is entirely accessible, in my view, to any law student or any lawyer. I think it is appropriate for us to understand that that kind of knowledge about the technology can be helpful and, indeed, increasingly is necessary to be effective in these areas.

AUDIENCE: Is there any place where that is written, computer technology for novices or lawyers?

MR. PERRITT: Well the ABA has published some materials. There is a book that's . . . got a title like *The Yellow Pages of Computer Basics for Lawyers.* The ABA law practice management section publishes that. I've got a couple of books out. My purpose is not to promote my books, but one that's published by PLI is about legal automation for legal institutions (*How to Practice Law with Computers*) and there's another, that's published by Wiley called *Law and The Information Superhighway* that's about substantive issues that arise from use of the technology.

MR. CHARNEY: If I may add, I really think it's important—I agree that this stuff is imminently learnable. But as someone who spends an inordinate amount of time unfortunately overseas on these issues, don't run the risk of oversimplifying how complex this is and the way it's changing the world, alright? Let me give you an example.

Remember about four years ago we were looking at massive health care reform and one of the possible health care reform approaches was a single-payer system that everyone would funnel into the Government and the Government would run a health care program. It was one of the options on the table. When that opinion was being discussed, I got a call from Don Perigoff. Don is my counterpart at the Canadian Department of Justice.

And Don comes down with the RCMP, the Royal Canadian Mounted Police, and he says I want to talk to you about health care. I said, "Okay, what about it?" He said, "In Canada, we have a national health care system." And I said, "I know this. You know, we're looking at it as a potential US model." He says, "Well we have fraud in the health care system."

This came as a complete shock to me. I couldn't believe it. So he says, "So we do all of these fraud cases." And I said, "Well, we do a lot of fraud cases." He says, "Well, we need medical records and insurance records." And I said, "We get medical records and insurance records." He said, "Well, we go to a system administrator who works for the Government who has all the records." And I said, "Well, you know, we've got VA hospitals but most of our providers are private and stuff."

He says, "Well, you know, even though we go to a Government provider, we have to bring a search warrant because of Canadian privacy law." And I said, "Okay, well, medical records are very sensitive. You know, we

have subpoenas and search warrants and stuff like that." He said, "But, you see, it occurred to us that we might be investigating a health care fraud case where the system administrator is involved in the fraud, maybe getting kick-backs or something."

And I said, "Well, that would be bad." He said, "Yeah, that'd be terrible because if we give the guy the search warrant, he'll destroy the records, we can't do that." I said, "No, you can't do that." He said, "So you see, what we've decided we would do is we would arrest the system administrator, and the Royal Canadian Mounted Police, they would get down and they would execute the warrant."

And I said, "Don, why do I care about this?" He said, "All of their records are stored in Ohio." I said, "You can't do that. You have no authority to execute a Canadian search warrant on U.S. territory." And he said, "They're my records." And I said, "Then you shouldn't have put them in my country. Why would you put the Canadian health care records in Ohio?" And he said, "You know, it's funny, but storage is a lot cheaper in Ohio than in Ottawa."

So when you start talking about this technology, it is learnable, but if you think these issues are simple, how do you enforce sovereign rules in a global Internet? The Germans and French are proposing contact regulations on the Net. Now in the United States we have a cherished First Amendment and we believe in free speech and we tolerate neo-Nazi speech. So do we tell the Germans, you have to tolerate neo-Nazi speech, too, because hey, it's on the web?

And if Germans are accessing neo-Nazi speech in the U.S., you've just got to live with it. They may not feel that way, considering their history. And what if another country said to us, "We think kiddie porn is really cool." So we've got all of these web sites and the rule on the global Internet, since everything is accessible everywhere, is the lowest common denominator. I don't think people are going to be feeling comfortable with that.

So the technology is imminently understandable, but if you think all of these issues will be resolved easily or without some very troubling weighing and balancing, you shouldn't, because these things are hard.

MR. PERRITT: I couldn't agree more. The effect is that the technology is diminishing further sovereignty in places where it traditionally has been found. Either governments of any kind will have diminished effectiveness or else there will have to be some new structures at the international level to deal with some of these things. That is a fundamental change and maybe even revolutionary.