POLICING THE INTERNET: *JAKE BAKER* AND BEYOND

March 9, 1995

SCOTT CHARNEY'S OPENING STATEMENT

March 9, 1995

SCOTT CHARNEY:

Let me give you a little perspective in ways some of the broad privacy issues that are involved in our day to day work at the Justice Department.

We're seeing an interesting interplay between the First and Fourth Amendment, and perhaps the most interesting and complex issue for us at the current time is the issue of comingling.

Basically, we see computers used for three legitimate purposes. They are storage devices, large storage devices. They are communications devices, both for real time chat sessions, electronic mail and file transfers. And with the advent of desk top publishing, they're publishing devices.

On the other hand in our daily work we see computers used in three different ways on the criminal side. Computers are often targeted by individuals, which means the actor's conduct is designed to steal information from or cause damage to a computer system.

They're also tools of the offense, which means that they're used to commit some traditional offense. In the old days, tellers used to take money from the till and stick it in their pocket. Now they write little programs to syphon off pennies from accounts and funnel it into another account, the so-called salami technique. You take thin slices off a big chunk.

And then we see computers what we call incidental to the offenses, which means they're not directly involved in the offense, but they're important to law enforcement.

Drug dealers are an example. In the old days, we'd get a search warrant, kick in the door, and if we did our job right, there would be white powder and currency and a little black book. And you opened up that little black book and you find names, dates and amounts.

Well, now you kick in the door and you find the powder and the currency and a stand alone PC.

And the reason that this is so significant to law enforcement is any federal agent can open up that black book, but I have to tell you not every federal agent should be turning on that computer. It could be that he's simply unaware of the programs that are running, the operations software. Maybe he knows Excel and it's running Lotus. Maybe it's been boobie trapped with time bombs. If you don't press the right keys quickly enough, data starts overriding. We had one case where there was actually an explosive device attached to the on-off switch. Fortunately the agent had unplugged the device from the wall rather than using the switch.

The critical issue Constitutionally is that one computer can be used for all these legitimate purposes and all these criminal purposes at the same time. The computer can be a weapon, and at the same time, be engaged in some publishing activity.

It is not uncommon, for example, for us to find bulletin board systems in which when you sign onto the board you get the publicly available information, such as information on the AIDS virus, where to go for treatment, recent test results for AZT.

But if you know the system administrator and get the special password you get kiddy porn copyrighted software and access devices.

When we go in and seize that computer, pursuant to Rule 41, we're shutting down the cracks.

So one of the big problems for us in the years ahead is commingling and how to treat computers that are used for these various purposes, do our job, but not infringe on the First Amendment rights.

The second thing we have to realize about the Internet and about these new networks is they're borderless. Countries are not yet ready to give up their sovereignty, but it is hard to determine how to do cases on the Net. Let me give you an example.

I have a counterpart in Canada and he came to see me, and he said, I want to tell you about our health care system, you know, we have national health care. And I said, yeah, we know a lot about that, we've been looking at your system. And he said, well, you may find this hard to believe, but sometimes there's fraud in the health care system.

(Laughter)

SCOTT CHARNEY: This came as a complete shock to me. And he said, you know, when we suspect fraud, we go to the system administrator for the health care system and we ask for medical records and billing records. And I said, okay.

And he said, you know, if we suspect it, we give them a search warrant, because they have to have paper before they can disclose, it's a privacy protection. I said, okay.

And he said, you know, if I believe the system administrator were involved in the crime, maybe getting kick-backs, we would not go to the system administrator, we would push the system administrator out of the way and the RCMP, Royal Canadian Mounted Police, would do the search.

And I said, Don, why are you telling me this. And he said, because all of our medical records are stored in Ohio. And I said, you can't do that.

(Laughter)

SCOTT CHARNEY: So one of the problems is to figure out how we're going to deal with this global network. Who's rules are going to apply? What level of privacy? France has stricter rules on transporter data laws than the U.S. does. Whose rules apply? Those things will need to be worked out.

The next problem, is that legislation is definitely going to be needed, and current legislation needs to be amended. The reason for that is that as we look at these new technologies, if we're going to regulate them in some way, if we're going to say a certain conduct is criminal, we absolutely must be clear in what we are prohibiting.

The problem is that it's easier to talk about these things, but when you actually sit down to write legislation, it's incredibly difficult.

No greater example can be found in the privacy in the work place bills; H.R.1900/S.984 of the last session. Congress has been looking at privacy in the work place for awhile because one of the things that this technology allows you to do is monitor all people all the time.

You can set up a program and then go to your secretary and say, you hit the backspace key seven times in the last twenty minutes, you're a bad typist, you're fired.

You can. I went to one technical conference where this company gave me a pen and they said, all our employees carry this pen, it tells us where they are in the building at all times. And I said, how about the bathrooms. They said, at all times. And I said, if I worked for your company, you would think I'm laying prone in the desk drawer, because that's where you'd find me.

(Laughter)

SCOTT CHARNEY: But it's mandatory if you want to work there.

So Congress devised these bills to protect privacy in the work place. And what they did was say, all monitorings prohibited, basically, unless it's part of a collective bargaining agreement or part of a bona fide service observation program, which means somebody's listening in to make sure you're giving the customer a courteous response in handling their request appropriately.

Well, they define the information to be protected as any information identifiable to any individual.

So when we met with them, I said, look, in the Justice Department we have distributed processing. I have a work station, but we have a server, and the server keeps copies of all my files in a directory called "NU.CHARNEY." So all those files are identifiable to me.

Since I do not have a collective bargaining agreement, and I'm not under a bona fide service observation program, that server now becomes illegal. Computers are banned.

This was not their intent. But it highlights how difficult it is to figure out how we're going to regulate this environment and define our terms.

I will leave you with one more example, well actually two more examples that are kind of related.

One is we have to recognize as we go to this national information infrastructure and global information infrastructure, we have to focus on the different types of things that we need to protect privacy for there is communicative privacy, our voice communications, our E-mail communications, our oral communications, and then there's the more sensitive right now issue of transactional privacy. More sensitive because wire tapping, voice wire or electronic communications is flat out illegal. It has been for a long time, since 1968.

But as we use this technology, we are creating more and more transactional data.

The classic example of this is the Intelligent Transportation System, or ITS. We can put a chip in your car and we can put receivers on every mile marker and then we tell you, this is great, if you break down and you hit a button on your dash board and the nearest garage is notified that you're between mile marker ten and eleven and you've broken down, and people go, we like that. And then you say, and you know what, if you're driving alone late at night and someone's following you, you press a distress button and then you see flashing lights, because there's a police car behind them. And they go, we like that.

And when you drive from Washington to New York you can get a letter three days later saying, you travelled two hundred miles in only two hours, you must have been speeding, attached is the ticket. They go, they don't like that. But it highlights the privacy problem.

One of the things we're going to have to decide and one of the critical issues, as we use all these technologies, to what extent are we going to build into these technologies anonymity and to what extent are we going to require accountability, because there are good reasons to have anonymity on the net. Whistle blowers want it, citizens just concerned about their privacy want it, the problem is, criminals want it. People up to bad things want anonymity, too.

So the problem is, if we create a network with complete anonymity, what happens not just in the criminal realm but in the civil realm when someone sends out 75,000 E-mail messages saying that their boss is a sexual pervert and mentally depressed. Where's the remedy if it's an anonymous communication?

Now, some people have said, well, we've had anonymous communications for years. We can send an anonymous mail. You can go to a pay phone and drop in a quarter and have an anonymous call. That's all true.

The problem is, that those technologies are one to one. Yes, I can call 75,000 people and tell them my boss is a pervert, but I need a lot of quarters, and I'll be standing out there forever. On the Internet, I can do it in half a second.

So we need to think very seriously about to what extent, as these new technologies come into vogue, we are going to demand accountability, anonymity or that middle ground, confidentiality, which means, your name is not associated with that particular message when it's delivered, but it's on file somewhere and with appropriate process someone can get access to it.

LOWENSTEIN: Next we will have Virginia Rezmierski from the University ITD.