

Connecticut Public Acts

HB 5041	PA 206	1984
House - 1996-2002, 2439-2448		(17)
Senate - 2089-2090, 2145		(3)
Public Safety - 63		(1)
(1983-84) Judiciary (Interim) subject of "Computer Crime"		
LAW/LEGISLATIVE REFERENCE	453-490 (38p)	59
DO NOT REMOVE FROM LIBRARY		2/P

Pages from the Hearings and Proceedings of the Connecticut General Assembly relating to a specific public act

Connecticut State Library
2012

CONNECTICUT
GEN. ASSEMBLY
HOUSE

PROCEEDINGS
1984

VOL. 27
PART 6
1894 - 2237

roll. Will the members please return to the Chamber immediately. The House of Representatives is now voting by roll. Will the members please return to the Chamber immediately.

DEPUTY SPEAKER FRANKEL:

Have all the members voted? Have all the members voted, and is your vote properly cast? Have all the members voted? If so, the machine will be locked, and the Clerk will please take a tally.

Will the Clerk please announce the tally.

CLERK:

House Bill 5572, as amended by House Amendment Schedule "A".

Total Number Voting	142
Necessary for Passage	72
Those Voting Yea	142
Those Voting Nay	0
Those Absent and Not Voting	9

DEPUTY SPEAKER FRANKEL:

The bill as amended is passed.

CLERK:

Calendar No. 249, File No. 336, Substitute for House Bill No. 5041, AN ACT CONCERNING COMPUTER-RELATED OFFENSES. Favorable Report of the Committee on Judiciary.

REP. COLEMAN: (1st)

Mr. Speaker.

DEPUTY SPEAKER FRANKEL:

The gentleman from the First Assembly District,
Rep. Coleman.

REP. COLEMAN: (1st)

Thank you, Mr. Speaker. I move acceptance of the
Joint Committee's Favorable Report and passage of the bill.

DEPUTY SPEAKER FRANKEL:

The question is on acceptance and passage. Will
you remark, sir.

REP. COLEMAN: (1st)

Thank you, Mr. Speaker. This bill attempts to
address a problem which is of growing concern. Last year
in this country it was estimated that U.S. companies
experienced about \$100 million in losses resulting from
computer crimes. This problem is of increasing concern,
not only to large corporations that rely upon computers,
but also to small businesses which rely heavily upon
computers.

Mr. Speaker, the Clerk has an amendment, LCO 2944.
May the Clerk please call the amendment, and may I be
permitted to summarize.

House of Representatives

Wednesday, April 18, 1984

DEPUTY SPEAKER FRANKEL:

The Clerk has LCO No. 2944, which will be designated as House "A". Would the Clerk call the amendment only.

CLERK:

LCO No. 2944, designated House Amendment Schedule "A", offered by Repl Tulisano of the 29th District.

DEPUTY SPEAKER FRANKEL:

Is there objection to summarization? Hearing none, you may proceed, Rep. Coleman.

REP. COLEMAN: (1st)

Mr. Speaker, the substance of this amendment was originally intended to be included in the bill, but was not through some oversight. The amendment merely makes clear that the State or a political subdivision may be a defendant as well as a plaintiff in a civil action brought to remedy a violation of this bill.

I urge adoption of the amendment, Mr. Speaker.

DEPUTY SPEAKER FRANKEL:

The gentleman's moved adoption of House "A". Will you remark on the adoption of House Amendment Schedule "A".

REP. JAEKLE: (122nd)

Mr. Speaker.

klc

96

House of Representatives

Wednesday, April 18, 1984

DEPUTY SPEAKER FRANKEL:

Rep. Robert Jaekle.

REP. JAEKLE: (122nd)

A question through you to the proponent of the amendment, please.

DEPUTY SPEAKER FRANKEL:

Please frame your question, sir.

REP. JAEKLE: (122nd)

What is the potential fiscal impact on municipalities by not having sovereign or governmental immunity available to them? Through you, Mr. Speaker.

DEPUTY SPEAKER FRANKEL:

Rep. Coleman.

REP. COLEMAN: (1st)

Through you, Mr. Speaker, Of course, there would be some impact if the State does gain access intentionally without authorization to computer systems. However, there would be no impact if the State does not violate the provisions of this legislation.

DEPUTY SPEAKER FRANKEL:

Rep. Jaekle.

REP. JAEKLE: (122nd)

So, through you, Mr. Speaker, there is a potential fiscal impact on the State and municipal governments?

House of Representatives

Wednesday, April 18, 1984

DEPUTY SPEAKER FRANKEL:

Rep. Coleman.

REP. COLEMAN: (1st)

I would say yes, there is a possibility of fiscal impact, but I think that possibility is minimal.

DEPUTY SPEAKER FRANKEL:

Rep. Jaekle.

REP. JAEKLE: (122nd)

Through you, Mr. Speaker, is there a fiscal note in connection with this amendment?

DEPUTY SPEAKER FRANKEL:

Rep. Coleman.

REP. COLEMAN: (1st)

I believe there is, Mr. Speaker.

DEPUTY SPEAKER FRANKEL:

Rep. Jaekle, I believe your question's been answered. Do you care to pose another question, sir.

REP. JAEKLE: (122nd)

I am wondering, through you, Mr. Speaker, if he could share with the members, certainly myself, what the fiscal note on the amendment says, through you, Mr. Speaker.

DEPUTY SPEAKER FRANKEL:

Rep. Coleman.

REP. COLEMAN: (1st)

There is an explanation of estimates at the end of the file copy, Mr. Speaker. It's File No. 336.

REP. JAEKLE: (122nd)

I'm sorry, Mr. Speaker. Maybe I'll be more specific. Is there a fiscal note in connection with the amendment known as LCO No. 2944? Through you, Mr. Speaker.

DEPUTY SPEAKER FRANKEL:

Rep. Coleman.

REP. COLEMAN: (1st)

Through you, Mr. Speaker, I apologize. There is not a fiscal note on the amendment.

REP. JAEKLE: (122nd)

Mr. Speaker, I'm not going to raise a point of order on a fiscal note, but what has happened in the past is items where a fiscal note is requested, and I'd certainly like to see a fiscal note. I'm wondering if this item might be passed temporarily or passed retained.

REP. GROPPPO: (63rd)

Mr. Speaker.

DEPUTY SPEAKER FRANKEL:

Rep. Groppo.

REP. GROPPPO: (63rd)

Mr. Speaker, I think the timing is perfect, and I

klc

House of Representatives

Wednesday, April 18, 1984

ask that this be passed temporarily and that the Clerk call the Order of the Day.

DEPUTY SPEAKER FRANKEL:

The motion before the Chamber is to pass temporarily LCO No. 2944, designated House "A". The motion to pass the motion temporarily will carry with the main motion to pass the bill. Is there objection to the motion to pass temporarily? Hearing none, the amendment and the bill is passed temporarily.

SPEAKER STOLBERG:

Are there any announcements or points of personal privilege at this time? Before we move to the Order of the Day. Are there any announcements or points of personal privilege at this time?

CLERK:

Calendar Page 1, Order of the Day for Wednesday, April 18, 1984. Calendar No. 369, File No. 425, Substitute for House Bill No. 5212, AN ACT MAKING APPROPRIATIONS FOR THE EXPENSES OF THE STATE FOR THE FISCAL YEAR ENDING JUNE 30, 1985. Favorable Report of the Committee on Appropriations.

REP. POLINSKY: (38th)

Mr. Speaker.

CONNECTICUT
GEN. ASSEMBLY
HOUSE

PROCEEDINGS
1984

VOL. 27

PART 7

2238-2645

kok

House of Representatives Thursday, April 19, 1984

retained from yesterday, Mr. Speaker. We had reached a point of discussion on House Amendment "A", at which point Rep. Jaekle inquired about the fiscal impact of the amendment.

I have a fiscal note now, and the explanation of estimates is as I had indicated yesterday. There would be some potential fiscal impact, but the simplest way to explain that is that if the state or any political subdivision violates the law, yes, there would be fiscal impact. If the state or any political subdivision does not violate the law, there would not be any fiscal impact.

Again, Mr. Speaker, I move the adoption of the amendment.

SPEAKER STOLBERG:

The Clerk has an amendment, LCO 2944, House "A". The Clerk please call the amendment once again.

CLERK:

LCO No. 2944, designated House Amendment Schedule "A", offered by Rep. Tulisano of the 29th District.

SPEAKER STOLBERG:

Rep. Coleman.

REP. COLEMAN: (1st)

Mr. Speaker, may I have permission to summarize the amendment again. I believe that was done. If you could

kok

House of Representatives

Thursday, April 19, 1984

briefly do that, and then move adoption, that would be appropriate.

REP. COLEMAN: (1st)

Briefly the amendment makes it clear that the state or any political subdivision could be a defendant as well as a plaintiff in a civil action for a computer crime. The defense of governmental immunity would not prevent such an action. I move adoption of the amendment, Mr. Speaker.

SPEAKER STOLBERG:

Will you remark further on the amendment? Will you remark further on the amendment? If not, --

REP. FARR: (19th)

Mr. Speaker.

SPEAKER STOLBERG:

Rep. Farr.

REP. FARR: (19th)

Just a question through you to the proponent of the amendment.

SPEAKER STOLBERG:

Please frame your question.

REP. FARR: (19th)

Did this amendment ever have a public hearing or was it ever subject to a public hearing, the issues in this amendment? Through you.

kok

House of Representatives Thursday, April 19, 1984

SPEAKER STOLBERG:

Rep. Coleman, do you care to respond?

REP. COLEMAN: (1st)

To my knowledge, the amendment did not have a public hearing.

REP. FARR: (19th)

I'll just comment. I guess the difficulty I have with the amendment is not the substance of it. It's just I wonder whether those parties who might be affected are aware of the substance of the amendment. And I'm a little bit concerned about the process.

REP. COLEMAN: (1st)

Mr. Speaker.

SPEAKER STOLBERG:

Rep. Coleman.

REP. COLEMAN: (1st)

May I defer to Rep. Tulisano. He may have a bit more information about the amendment.

SPEAKER STOLBERG:

Rep. Tulisano, do you accept the yield?

REP. TULISANO: (29th)

Yes, Mr. Speaker. Mr. Speaker, it is clear that the intent of having the municipalities involved, was the subject

in one of the drafts. It was one section that was there. When the final draft came out, and everybody was aware that this was part of the process. In fact, there was testimony from interested parties, that should be included. And obviously myself included.

There was interpretation, that in the introductory paragraph when a person is defined to include any municipality in the definition, that this would cover this particular system of provision. However, on thought, we think you need something more specific on that to properly draft the legislation because of the other, like the Claims Commission statutes that are on file, and that's why it's being done as an amendment now.

SPEAKER STOLBERG:

Will you remark further on the amendment? If not, all those in favor of the amendment, please indicate by saying aye.

REPRESENTATIVES:

Aye.

SPEAKER STOLBERG:

All those to the contrary, nay.

REPRESENTATIVES:

No.

kok

House of Representatives

Thursday, April 19, 1984

SPEAKER STOLBERG:

The amendment is adopted and ruled technical.

House Amendment Schedule "A".

After line 253, insert a new subsection (9) as follows and renumber the remaining subsection accordingly:

"(g) A civil action may be brought under this section against the state or any political subdivision thereof and the defense of governmental immunity shall not be available in any such action. The rights and liability of the state or any political subdivision thereof in each such action shall be coextensive with and shall equal the rights and liability of private persons in like circumstances."

SPEAKER STOLBERG:

Will you remark further on the bill? Rep. Coleman.

REP. COLEMAN: (1st)

Mr. Speaker, the Clerk has an amendment, LCO NO. 3711. May the Clerk please call that amendment, Mr. Speaker, and may I be given permission to summarize.

SPEAKER STOLBERG:

The Clerk has an amendment, LCO 3711, designated House "B". Will the Clerk please call.

CLERK:

LCO No. 3711, designated House Amendment Schedule "B", offered by Reps. Tulisano, Coleman and Farr.

SPEAKER STOLBERG:

Rep. Coleman has asked leave to summarize. Is there objection? Seeing none, please proceed.

REP. COLEMAN: (1st)

Mr. Speaker, this amendment does two things. First of all, it does not change the intent of the penalty section but it does change some of the language of the penalty section to make the description of what would constitute a class A misdemeanor, and a class B misdemeanor more clear and more consistent with the preceding language of the section.

Secondly, the amendment would clarify some venue considerations. Presently the bill provides that the state would have jurisdiction, if an act that's prohibited by the bill takes place in the state or if equipment that is illegally accessed is located in the state, the state would have jurisdiction over that matter, but it does not indicate which town would have jurisdiction to bring the prosecution.

The amendment clarifies that by giving the state the option of bringing the action, the prosecution, either where the act occurs or where the equipment is located. I move the adoption of the amendment, Mr. Speaker.

SPEAKER STOLBERG:

Will you remark further on House "B"? If not, all

those in favor of the amendment, please indicate by saying aye.

REPRESENTATIVES:

Aye.

SPEAKER STOLBERG:

All those to the contrary, nay. The amendment is adopted and ruled technical.

House Amendment Schedule "B".

In line 130, delete the words "does not exceed one" and substitute in lieu thereof the words "exceeds five hundred"

In line 131, delete the word "thousand"

In line 138, delete the words "does not exceed" and substitute in lieu thereof the word "is"

In line 139, after the word "dollars" and before the period insert the words: "or less"

After line 179, add section 11 as follows and renumber the remaining sections accordingly:

"Sec. 11. (NEW) (a) In any prosecution for a violation of section 2 of this act, the offense shall be deemed to have been committed in the town in which the act occurred or in which the computer system or part thereof involved in the violation was located.

(b) In any prosecution for a violation of section 2 of this act based upon more than one act in violation thereof, the offense shall be deemed to have been committed in any of the towns in which any of the acts occurred or in which a computer system or part thereof involved in a violation was located."

SPEAKER STOLBERG:

Will you remark further on the bill? If not, will members please be seated. Staff and guests come to the well of the House. The machine will be opened.

CLERK:

The House of Representatives is now voting by roll.
Will the members please return to the Chamber immediately. The House of Representatives is now voting by roll. Will the members please return to the Chamber immediately.

SPEAKER STOLBERG:

Have all the members voted? Have all the members voted and is your vote properly recorded? If all the members have voted, the machine will be locked and the Clerk will take a tally.

Will the Clerk please announce the tally.

CLERK:

House Bill 5041, as amended by House Amendment Schedules "A" and "B".

Total number voting	143
Necessary for passage	72
Those voting yea	143
Those voting nay	0
Those absent and not voting	8

kok

211

House of Representatives

Thursday, April 19, 1984

SPEAKER STOLBERG:

The bill is passed.

CLERK:

Calendar page 12, Calendar No. 254, File No. 364, Substitute for House Bill No. 5675, AN ACT CONCERNING STANDARDS FOR THE OPERATION OF CERTAIN SOURCES OF NON-IONIZING RADIATION. Favorable Report of the Committee on Environment.

SPEAKER STOLBERG:

Rep. Moynihan.

REP. MOYNIHAN: (10th)

Mr. Speaker, might that item be passed, retaining its place on the Calendar.

SPEAKER STOLBERG:

The motion is to pass, retain. Is there objection? Is there objection? Seeing no objection, it's so ordered.

CLERK:

Calendar No. 266, File No. 383, Substitute for House Bill No. 5082, AN ACT ALLOWING EXTENSION OF TIME FOR PAYMENT OF SUCCESSION TAXES WHEN AN ESTATE CONSISTS PRIMARILY OF WORKS OF ART OF THE DECEDENT. Favorable Report of the Committee on Finance, Revenue and Bonding.

REP. SMOKO: (91st)

Mr. Speaker.

SPEAKER STOLBERG:

The distinguished Chairman of Finance, Ron Smoko.

CONNECTICUT
GEN. ASSEMBLY
SENATE

PROCEEDINGS
1984

VOL 27

PART 2

1838-2355

Regular Session
Thursday, April 26, 1984

Page 152
jgt

bill as amended, Senator?

SENATOR OWENS:

That allows the validating of the filing of the notice of Alberto Ocasio and it allows it to be heard by the Commissioner on Claims. I'd ask, if there's no objection, that this bill as amended by placed on consent.

THE CHAIR:

Any objection to placing the bill as amended on consent? Hearing no objection, the matter will go on consent.

THE CLERK:

Page 13, calendar 515, Files 336 and 762, Substitute for House Bill 5041. An Act Concerning Computer Related Offenses. (As amended by House Amendment Schedules "A" and "B"). Favorable Report of the Committee on Judiciary.

THE CHAIR:

Senator Owens.

SENATOR OWENS:

Mr. President, move acceptance of the joint committee's favorable report as amended by House Amendment "A" and House Amendment "B" and passage of the bill. House Amendment "A" permits a private law suit to be filed against the state or municipality in violation of the law. House Amendment "B" specifies in which town or towns a computer crime would be deemed to have occurred. Move adoption of both of these amendments please.

THE CHAIR:

Will you remark further? All those in favor signify by saying aye. Opposed, nay. The ayes have. Remark on the bill as amended.

SENATOR OWENS:

Yes. It would make the following activities a computer crime: unauthorized access to a computer system, theft of computer services, interruption of computer services, misuse of computer system information and destruction of computer equipment. I'd ask, if there's no objection, that this bill as amended by House Amendments "A" and "B" be placed on consent.

THE CHAIR:

Any objection to placing on consent? Hearing no objection, the matter will go on consent.

THE CLERK:

Calendar 516, File No. 480, Substitute for House Bill 5874. An Act Concerning The Notification Of The State Of The Formation, Alteration and Termination Of Special Districts. Favorable Report of the Committee on Planning and Development.

THE CHAIR:

I believe Senator Wilber Smith has left the chamber on legislative business. I think if there is no objection, we'll pass retain that matter. Any objection? Hearing no objection, we'll move on to the next item.

THE CLERK:

Calendar 517, File No. 556, Substitute for House Bill 5752. An Act Concerning The Distribution Of Drugs To Medical Practitioners. Favorable Report Of the Committee on Public Health.

THE CHAIR:

Senator Regina Smith.

THE CHAIR:

Please give your attention to the Clerk who will list the items that will be on the second consent calendar for today. Give your attention to the Clerk please?

THE CLERK:

On page 3, calendar No. 347. On Page 4, calendar 385. Turning to page 12, calendar numbers 511, 512, 513, 514. Page 13, calendar numbers 515, 517, 518. On page 14, calendar No. 522. On page 23, calendar No. 65. On page 24, calendar No. 148. On page 26, calendar numbers 367, 523, 524, 525. On page 27, calendar 526. On page 28, calendar 273. That completes the list of items on the second consent calendar.

HB5066-11B5416
HB5413-11B5546
HB5041-11B5072
11B5571-11B5621
SB223-SB265
CT25-HT21
HT26-HT28
HT24-SB341

THE CHAIR:

Is there any question of any item listed on the consent calendar. Is there any objection to any item on the consent calendar? Hearing none, the machine is open. Senator O'Leary. Machine'll be closed and locked. Total voting is 34, voting yea is 34. The consent calendar is adopted. Senator Schneller. Excuse me. Senator Larson.

SENATOR LARSON:

Thank you, Mr. President. Just a very brief reminder to everyone in the circle. Tomorrow we face a very stiff test. A lot of our reputations are on the line as baseball players. I hope all of you will make it to the fine Community of East Hartford tomorrow evening. Try to get there about 4:30. We haven't had any practice except a few coin flips. That's how we won last year's game, but if you could get there about 4:30, we've got a team pitcher that's scheduled for five o'clock, so at least make sure

**JOINT
STANDING
COMMITTEE
HEARINGS**

**PUBLIC
SAFETY
1-296**

**1984
INDEX**

MS. KRUPENEVICH: (continued)

legislature that consumers share with legislature in the cost of this program. Initial cost to legislature over a three year period will be about \$6.6 million in order to begin implementation of the program. To the consumer implementation of this program will result in an increase of about .40 a month on their telephone bills for the first three years then will decrease to less than 1.5 cents a day. While advocating the enhanced 911 system as an added measure of safety for all, particularly the handicapped and elderly. One issue of concern is an individual's rights to privacy.

If Connecticut implements enhanced 911 how do we know data isn't going to be tampered with. One of the biggest fears of the handicapped population and elderly or anybody is that of theft, muggings, break-ins etc. The state Judiciary Committee has before them a working draft of a bill, An Act Concerning Computer Related 305011 Crimes which would mandate that there be certain security requirements implemented in government and industry for computers. This is being addressed this legislative session. The Hartford Advisory Commission on the Handicapped supports implementation for the 305011 enhanced 911 system.

Within the City of Hartford there are approximately 20 group homes and community training homes which serve about 100 clients. Statewide there are over 450 group homes and community training homes serving approximately 700 clients. If the basic 911 system was implemented in Hartford 21.4% of Hartford's residents would not receive this service. Areas affected would include the West End, Charter Oak and Albany areas. The need for enhanced 911 is imminent in order for all of Hartford and Connecticut to be given this added measure of safety.

As opposed to the basic 911, which provides services to some towns and then only portions of others, the enhanced 911 system will provide emergency services to all of Connecticut regardless of geographical or telephone exchange boundaries. Thank you for your time.

SEN. AVALLONE: Are there any questions? (inaudible)

**JOINT
STANDING
COMMITTEE
INTERIM
HEARINGS**

**JUDICIARY
PART 2
395-739**

1983-1984

1
klu

JUDICIARY

State Capitol
Judiciary Room
December 5, 1983
2:00 P.M.

PRESIDING CHAIRMEN: Senator Owens
Representative Tulisano

COMMITTEE MEMBERS PRESENT:

SENATORS: Owens, Dorr

REPRESENTATIVES: Tulisano, Schlesinger, Chase,
Rybak, Berman, Wollenberg, Baronian,
Samowitz

Computer Crimes

REP. TULISANO: We'll call this public hearing dealing with
Cass 1 computer related crimes to order. We have an invited
speaker's list and of course, the public will be entitled
to speak. Starting with Rusty Post, Russell Post, Esquire
and former State Senator and a former member of this
Committee which makes his welcome even more, especially
warm for us. We love ex-members of the Judiciary Committee.
That means they're not competing with the present members.

MR. POST: Representative Tulisano, Senator Owens and members
of the Judiciary Committee, it's a pleasure and fun to
come back and catch up with you. Several months ago, a
group of us thought that this might be the year the
Judiciary Committee and the legislature as a whole, would
be concerned about the issue of computer crime and that
perhaps it would be helpful if people who have expertise
in that area could get together and use the extent of the
problem and do some drafting as an assistance to the
Judiciary Committee and as a result, a group of us did
get together, approximately half of whom are here at the
table, with me, and I'd like to kind of introduce them
to you and just explain a little bit about who the
Committee is, very briefly.

To my far right is Fred Brunetti from the Telephone
Company, Ian McQuire from Aetna, Bob Jerome from Travelers,
Linda Smittie who is a lawyer from the firm of Cummings
and Lockwood, and a partner who has great expertise in the
area of computer and computer losses and Anita Loalbo from

2
klu

JUDICIARY

December 5, 1983

MR. POST: (continued)

CBIA; Bob Johnston from Phoenix, Philip Luckhart from GE, and Jim Smittie who also is with Cummings and Lockwood with Linda and specializes in the field of computer losses.

We got together with some different people who couldn't be here today from other companies, Perkin-Elmer, IBM, Connecticut National Bank, Connecticut Bank and Trust, Dick Blumenthal a former U. S. Attorney, Austin McQuigan, the Chief State's Attorney, United Technologies. Austin is now with us, a little late, but you know--and what we wanted to do was to review the area of computer crime to see if legislation might be warranted and if so, to draft a proposal for your review and the Committee met to do that and the people who are here today are in a position to share with some of their concerns and the need for legislation in this area and some of the problems which today are not covered by Connecticut law.

And then secondly, Linda Smiddy who has review the legislation in the other states and pending at the federal level, drafted the legislation that this Committee has been studying for the last couple of months, can then kind of explain to you the process wherein and where that draft now stands, a copy of which we have for the Committee.

It is our plan and we hope to be able to accomplish this, to meet, draft and review and submit to the Judiciary Committee, our best draft, our best thinking on this concept by the end of 1983. In other words, by the end of this month, so that the Judiciary Committee can continue to review that and perhaps work on it prior to the session if you chose and then to make the people here that are a part of this committee, available to you, the Judiciary Committee, as a resource should you have additional questions or should you have additional thoughts and want to check them with the people who are part of this committee who have enormous expertise in the whole world of computer, computer law, computer crime, etc.

So with that, perhaps Linda, you can explain where we are and ask some of the people who are here to describe their areas of concern and following that, describe the legislation and what we think might be advisable for Connecticut.

3
klu

JUDICIARY

December 5, 1983

REP. TULISANO: Do you want to play musical chairs or musical mikes?

MR. POST: Whatever is easiest for you.

MR. TULISANO: Musical chairs would probably be easier.

MS. LINDA SMIDDY: Thank you. We thought it would be appropriate to begin our discussion by letting you hear comments from the various members of our committee who as Rusty said, have provided our committee with valuable input on the finer scope of the problem and the major issues which confront us, in connection with the problems related to computer crime.

First, I would like to turn to Anita Loalbo who is with CBIA and she is going to discuss the scope of the problem.

MS. ANITA LOALBO: Members of the Judiciary Committee, my name is Anita Loalbo. I'm Assistant Counsel for the Connecticut Business and Industry Association. We represent approximately 6300 firms which employ over 700,000 men and women in Connecticut and our membership ranges from large industrial and commercial corporations to small manufacturing and retailing businesses. My job today is to tell this Committee about the scope of computer crime as we see it in Connecticut. I'm sure those remarks will be fortified by those of Mr. McQuigan and other members of the Committee.

I think at the outset, it's important to emphasize that the problem that we face in Connecticut is one for obviously, for the larger corporations in Connecticut, but also for the very small companies in Connecticut which are reliant on the computer in today's business market and so it's on behalf of our entire membership that I come before this Committee. As a member of this panel, to discuss with you an area of concern to the business community in Connecticut.

The issue we're here to discuss is called computer crime and that issue is a broad term which includes and encompasses intentional theft, sabotage, destruction, manipulation, changes of vital computer information.

4
klu

JUDICIARY

December 5, 1983

MS. LOALBO: (continued)

You're going to hear today, from various members of this panel on specific instances and technical instances which I'm not going to be able to tell you about since I'm not a technical expert in the area of computers and it probably would be best, if the Committee has questions, to wait until people have spoken on specific areas before they begin to ask specific questions.

What I'm here to tell you today is that many of our member companies have expressed concerns through phone calls and through letters, over the issue of computer crime and they have requested that CBIA, along with the rest of the group, aid in the adoption of legislation which will set criminal and civil sanctions in Connecticut specific to crime associated with computers.

We have had many calls at CBIA to report computer problems over the last several years. The issue that the Association has learned this year, is an extremely sensitive one because it's computer based. It is not one that the business community has been very vocal on. There are several illegal activities which are implemented and achieved with computers and computer time. Connecticut businesses are not exceptions to the illegal activities that have been going on with computers and as this new technology becomes more and more commonplace in the business market, of all sizes, the issue becomes more and more critical to us all.

I can go briefly through the types of complaints that have been aired to CBIA through our membership to, for example, myself. Without specifying company names, or the types of business, there are several types of crimes that we hear over and over that are implemented in Connecticut. The most frequent is interruption or theft of computer services. For example, intentionally tying up phone lines so that people cannot have access to business. It's a very, very common problem. There is actual destruction of physical property, the computer itself, and/or what they call the intellectual property, the information and when we talk about altering information, we're talking about things such as erasing information, changing information, altering information, stealing

5
klu

JUDICIARY

December 5, 1983

MS. LOALBO: (continued)
information, all those kinds of crimes to what they call the intellectual property.

Another area is one that this Committee has looked at in-depth and that is unauthorized access to computers and there's a two-fold problem with unauthorized access to computers and I think you'll learn more about that and we're talking about unauthorized access from outsiders into a company and from insiders inside a company accessing a computer when they're not authorized to do so.

There are problems with embezzlement and fraud and the use of telephone lines and finally, there's a problem of disclosure of confidential information once it's obtained through some sort of means and disclosure through the high-technology means or from one custom to another.

And so those are the basic areas I think that this panel is looking at and all of these areas are of concern and have provoked calls to CBIA, so we know that there is a problem.

The use of computers, as I mentioned before, is becoming more and more commonplace in the business market. Very small companies use computers. My father has a company which is a small drugstore and he uses computers to phone in orders, to receive his orders, to check his inventory and that's just one small store that maybe employs a dozen people. The essential problem that the business community faces today in terms of computers, is that the existing criminal statutes or the existing civil statutes do not--are not adequate to prosecute an individual or individuals for crimes, specifically committed with, by, for or how a computer. And I think that today, what we're here to ask you to do is look at the problem very carefully. You're going to hear about what's going on the federal level and in different states and look to implement something in Connecticut which will help solve this in all businesses, both large and small.

MS. SMIDDY: Ladies and gentlemen, I would like to now ask Brian Maguire from the Aetna Insurance Company to speak to you about the problems at Aetna. Mr. Maguire.

6
klu

JUDICIARY

December 5, 1983

MR. BRIAN MAGUIRE: Mr. Chairman, my name is Brian Maguire. I'm a Counsel with Aetna Life and Casualty. As you may know, Aetna is a very large company. We have an awful lot of computers. We have them, not only spread throughout this country, but a good part of the world. A lot of them are linked together. We've had, in one case recently, which is symptomatic of the problem, we had a claims processor in Seattle whose job it was to take claims from large employers whom we insure, and process them through our system and see that they are paid and recorded for.

She and several cohorts decided to add herself and them to a list of insureds at one of the major companies that we insure and this then started to process false claims for themselves. They would actually have a computer generate a claim and a check and they would cash it and pocket the money. This scam resulted in \$370,000 loss to the company. They were discovered by an internal audit, prosecuted in the federal courts and are presently serving time in the federal penitentiary out in the west.

One of our concerns since it seems like justice had its day in that case, is that if their scam had a different objective or had not resulted clearly in the taking of money or other valuable property, our prosecution of that may have been thwarted. This is a problem that many companies in other industries are presently having.

Some computer crimes are not always technological and complex. In 1980, the Los Angeles Daily Journal, for example, reported that a large insurance company was a victim of electronic vandalism. After being fired, an irate ex-employee strolled through the main computer room with a powerful electro-magnet and destroyed an estimated \$10 million in computer software programs in that particular system. It doesn't say in the article, but very possibly they had to prosecute someone of that sort for some crime of vandalism. I would imagine that the penalty for that type of vandalism under existing statutes, would not anywhere be close to the damage to the employer.

While at Aetna we take great pains to secure our many

7
klu

JUDICIARY

December 5, 1983

MR. MAGUIRE: (continued)

computers and our systems and our networks, we are not immune to computer crime. It's not coincidental that we are here today to inform you of the need for computer legislation at a time when insurers, not only Aetna, but other major insurance companies, are spending millions and millions of dollars in programs to not restrict their computer accessibility, but rather to broaden it so make our in-house large computer system more available, more readily available, to independent agents throughout the country so that they can better serve our policyholders.

And so in fact our exposure to this kind of crime will continue to increase. The increased service opportunities require additional vigilance on our part, not only to protect our resources, but also to protect the privacy of our policyholders. We are concerned that when people use the technology available, to steal or damage our resources or invade the privacy of our policyholders, the present state law will not be adequate to provide appropriate remedies.

That is the present state law may not respond very neatly or very appropriately. We feel that the legislation under consideration by both our committees today would be effective in closing some of the criminal and civil loopholes that presently exist in our law. Thank you.

MR. ROBERT TYRRONE: Mr. Chairman, I was asked to volunteer some additional information. I would guess that at the present time, there might be at least 15,000 people who have access to that. 15,000. Hopefully that will grow if the balance of our programs works out, but it's a large number. Thank you.

MS. SMIDDY: Members of the Judiciary Committee, I would next like to introduce Robert Tyrrone who is with the Data Processing Department of the Travelers Insurance Company and he will talk on--specifically about how some of the crimes do occur.

MR. TYRRONE: Mr. Chairman, members of the Committee, my name is Bob Tyrrone. I'm with Travelers Insurance Company in the Data Processing Department. I'd like to talk about

MR. TYRRONE: (continued)

the evolution of the electronic bulletin board system which probably you have seen in some national publications and in local newspapers.

In the near future, there are expected to be 10 million home or personal computers; 2 million of these computers will have communications capability. The bulletin board system is a program which runs on a personal computer and it answers the telephone, establishes connectivity with another computer and offers a menu of options to the caller. These options allow the caller to read messages left by previous callers; receive private messages; transfer data and programs and other options.

During the late 70's, the bulletin board systems were used mostly by computer enthusiasts and user groups. Subject, they were generally run and maintained by an individual at his home. The information exchange was technical in nature and related to computers in general. By late 1981, the bulletin board proliferated on Apple, Atari, Radak and other personal computers. Subject matters on these bulletin boards have become diverse in nature and covered topics such as geneology, radio engineering, medical, astrology, photography and others.

One particular bulletin board system in New Jersey kept updated listings of all the bulletin boards in the world. With the entry of IBM into the personal computer market, bulletin board systems took another major advance in the world of TC. Coming on the scene were the pirate bulletin board systems. These address, discuss, disclose, the various copy protection schemes and used within the software industry. Information then appeared on these boards indicating the existence of bulletin boards devoted to phone freaking and computer hacking. A computer hacker is someone who spends time trying to gain access to computers, especially ones restricted to authorized users only.

A phone freaker is someone interested in making use of long distance facilities without incurring costs. These bulletin boards became an information exchange on breaking into many different computers, government, college, business and others. Access codes, phone numbers and

9
klu

JUDICIARY

December 5, 1983

MR. TYRRONE: (continued)

passwords were posted for use by any caller. Techniques for breaching security programs which searched phone exchanges for computers and hacking programs were also available. Specialists for package switching systems such as Telenet and Timenet divulged access information. Duck equipment specialists also participated. People who once had authorization to computers left access information such as valid account numbers in passwords.

By July of 1983, most of all hacking information could be found on the bulletin board in New York named O-Sunny. That stands for the Ohio Scientific Users of New York. Active hackers throughout the nation would post their findings here. The information gave computer neophytes step by step instructions of phone numbers, information to be answered, passwords, account numbers, to gain access to numerous computers.

Messages also began appearing warning of federal and phone authorities monitoring OSUNY with rumors of hackers being arrested. August brought the news of the arrest of a group of Michigan teenagers known as 414's; 414 being the phone code for the state of Michigan, who breached security of the government computer on the Telenet network. An article published in the September 30th issue of Newsweek dealt with computer hacking and disclosed the existence and nature of OSUNY. The 414's obtained the access information from that bulletin board system.

That same week, OSUNY and other hacking bulletin boards ceased to operate. The phone numbers were reported and disconnected. Shortly thereafter, they began to reappear. However, access to this hacking information is now restricted. Users were required to give their real name and address for clearance. This would reduce the possibility of federal and phone authorities for monitoring an activity. The trend has been established, therefore, that hacking bulletin boards have gone underground.

Today, the majority of bulletin boards and there are over a thousand of them, are used by personal computer users, home computer owners, to gather and disseminate a variety of information. Sensitive access data is not and probably

MR. TYRRONE: (continued)

will not be available on the scale it was during the first half of 1983. However, even though casual hacking has been minimized, the determined hacker, will give and get information on the underground bulletin boards where hacking capabilities reached very sophisticated levels. Personal computers, accessing other computers, will increase dramatically. Legislation should recognize the wealth of information on bulletin board systems that will benefit business, government, education and the private sector.

The possibility of sensitive access information reaching the general public has been reduced by the action of the federal authorities. The trend towards responsible use of personal computers has begun and should continue with farsighted legislation encouraging the use of and outlining the abuse of this modern device. Thank you.

MS. SMIDDY: Mr. Chairman and members of the Committee, I would next like to introduce Phil Luckhardt who is with the General Electric Corporation.

MR. PHIL LUCKHARDT: Thank you Linda. Mr. Chairman and members of the Committee, I appreciate the opportunity to discuss some of the concerns of GE which I believe are representative of the concerns of many multi-national companies who have our headquarters in Connecticut.

As you aware, GE is a worldwide manufacturer of services and technology company headquartered in Connecticut. We also have several of our major operating units with principle facilities in the state. The full employment in the State of GE, is about 7,000.

Like many industries operating in competitive markets, we have become increasingly reliant on computers. This is a matter of necessity, not luxury. To maintain our market position and our employment level, our general business good health, we have to use the efficiencies of the computer which it can give us. The range of users of the computer is broad; from research and development and technology to product design, manufacturing operations, control, board of entry shipping and billing, the general

11
klu

JUDICIARY

December 5, 1983

MR. LUCKHARDT: (continued)

financial accounting, applications, special financial applications, our credit operations and GE, of course, is an operator of a service bureau throughout the country.

The trend of all operations is to increasing use of communications. More and more, we are becoming linked, computer to computer, across the country and around the world. This is necessary to keep our credit and market position. By doing this, however, we greatly increase our exposure to detrimental access and unlimited and unwarranted use of our computers.

Our overall position on protection of computer systems in the company is that it is first-off, our own responsibility. We have instituted a corporate line program that delegates responsibility to our various operating units and provides guidelines to them to provide the kind of protection that is reasonably attainable. However, there is no such thing as 100 percent foolproof systems. The scope of our program covers communications, physical systems, information on the systems and personnel activities.

Again, we recognize this as our company's first line of defense. One of the types of information that we do want to protect in this is the employee, privacy information, that is maintained in our computers. We have a privacy program that parallels the federal program. Our own program was instituted voluntarily in an effort to look after the interest of our employees.

Regarding the crime legislation that is being discussed today, we do feel there is a need. We have had several instances of mischievous disruption; hackers coming in and in some cases, disgruntled employees who have left; where the intent is not necessarily arsonist, but to disrupt operations and this can be extremely damaging in some of our operations where the whole factory may have to shut down or it won't be able to ship a week's work in production if the computer is not available. We are also interested in protection for what we have defined in our task group as informational crime which would make a criminal offense out of disclosure of information obtained

MR. LUCKHARDT: (continued)

on an unauthorized basis from the computer. Theft of services is another area that we are concerned about and of course, destruction of computer equipment and unauthorized access. We feel that these problems do merit responsible attention. Again, since we are multi-national, we are headquartered in Connecticut, we have a special interest in what is done in the state to protect our headquarters' information along with the operating information both at home and in state. Thank you.

MS. SMIDDY: I would next like to introduce Mr. Robert Johnston who is with Phoenix Mutual Insurance Company and who will speak about the problems of computer time from the perspective of a smaller company.

MR. ROBERT JOHNSTON: Representative Tulisano and Senator Owens and members of the Judiciary Committee, I'm Robert Johnston of the Phoenix Mutual Life Insurance Company. I have eleven plus years of experience in the field of computers and I am a frequent speaker and writer on this subject area. I write a monthly column in the Medical Assistance Magazine which is a trade journal publication.

If you haven't learned it already, you're going to find out the statistics that are available on computer crime are unreliable. And you can go to any one of a number of sources and find the most noted of all being Don Clark's and in a recent article of his, published in the Computer Security of the Spring of 1983, he explained why they are unreliable, primarily because so many cases are not reported and as a result, we only have information based on that which is known and as we well know, statistics are not very beneficial when they are only based on what is known as opposed to what is reality.

So, why are we so concerned? Even with what is known, there is one major factor we cannot ignore and that is the average size of the known crime. Now, it's exceeding \$450 million. Granted, that's been skewed by some of the larger cases of the last few years but we can't ignore such a sum. And that's what's concerning all of us.

Legislative action is necessary not only to provide major

13
klu

JUDICIARY

December 5, 1983

MR. JOHNSTON: (continued)

companies a vehicle for prosecution on such systems as may arise, but also for the many smaller companies that cannot afford the available commercial protection. There are commercial solutions that will protect most of us in major instances, not one hundred percent, as was brought out a moment ago, but the fact is that most of the smaller companies can't afford this and they need some other form of deterrence to insure that they are also rightfully protected.

Small business is the whole name of the game. Other concerns, particularly of the larger companies which hasn't been mentioned so far, is the theft of resources which, for any major company that has a large number of computers, after all, wouldn't it be nice to connect your Apple to an IBM 30-33 and make your Apple have all the power of a 30-33? That's one of the fun games that goes on. You give all those resources available so another concern that we have is the theft of computing resources.

The concern from private industry has grown and is clearly demonstrated by the National Security Computer Conference in November in New York City where the attendance was up 40 percent this year. Legislative support is now needed as a deterrent to what private industry is trying to do.

MS. SMIDDY: Mr. Chairman and members of the Committee, I would now like to introduce Fred Brunetti who is with Southern New England Telephone Company and will present the perspective of the communications industry.

MR. FRED BRUNETTI: Mr. Chairman, members of the Committee, the Southern New England Telephone is the primary provider of telephone service in Connecticut, certainly supports the enactment of computer crime legislation. SNET is interested in preserving confidentiality of employee information which is presently contained on computers and in its computer systems. SNET is concerned about preserving the confidentiality of customer information presently read into computers. That includes non-published telephone numbers, includes toll billing records and it also includes telephone credit information. SNET is also concerned about protecting the confidentiality

MR. BRUNETTI: (continued)

of its commercial information. The telephone industry becomes competitive, a pervasive contained on SNET computers could work to SNET's commercial disadvantage if it were disclosed to third parties.

But most importantly, SNET is concerned about protecting the integrity of its telephone network. SNET's telephone network is in fact, for the most part, a computer network. The central offices, the electronic switching systems, that switch calls throughout the state, are indeed, computers containing programs and the other conditia of computer systems. In appropriate activities, directed at these central offices, could result in an interference with our billing systems. It could cause a disruption of certain network based services such as total phone service and touch tone service and in the worst case, inappropriate activities by hackers and others, could cause a disruption to all of the telephone service in a particular exchange.

Now, SNET is working constantly to reduce the risk of this kind of event occurring. SNET historically has worked with AT&T and the Bell System in that regard and will continue to work to protect the equity of its network. But SNET is against its efforts that would be well supported by a kind of legislation that we're talking about today. Thank you.

MS. SMIDDY: Mr. Chairman, and members of the Committee, you've now heard the members of our committee speak to identify the scope of the problem and some of the major concerns. You are now being handed a draft of the proposed legislation that ~~our~~ committee has been working on since September of 1983. The proposed draft also has attached to it, a brief summary of who the members of the committee are; an identification of some of the types of computer crimes that we have identified and discussed and attempted to deal with in our legislation as well as a brief summary of the methodology used by the committee in drafting this proposed legislation.

Now, I want to emphasize that this is what the committee describes as a working draft. We are still in the process

MS. SMIDDY: (continued)
of analyzing and revising the draft as it now stands.

SEN. OWENS: Could I just ask you a couple questions, Attorney Smiddy? I've done a little research on my own, not, you know, to find out what other jurisdictions have done. I've spoken to some professors at Harvard and so forth and the usual thing that we do. Basically, what are the pitfalls since the United States Government--and obviously, they haven't adopted a law in the United States Code with respect to this and they've had a lot of problems in it--in drafting anything and most of the states are unable to come up with a draft. What are the real problems or what are the pitfalls in this type of legislation?

Why is it so hard? In other words, what are they afraid-- in other words, where--and I commend you. You're courageous to--you're getting into what's almost an unchartered area when we start talking about drafting something like this. What are the pitfalls and what are the problems that these other jurisdictions have had in coming up with legislation like this?

MS. SMIDDY: As you know, about 15 states have enacted legislation. I think one of the main problems with coming up with--are the problems are two-fold. One is simply gathering together people who can identify what the problems are, what the crimes are. We've heard references to the problems but I think that frequently people who are not directly involved with computers or with the use of computers, do not always imagine how these problems can occur and the second problem is, of course, that we're dealing with a highly technical area and once again, we are attempting to define in language that we can all understand, what the problems are related to crimes which are based on a technology that many of us may not be familiar with at all.

SEN. OWENS: Just along the same lines, what states have enacted legislation like this?

MS. SMIDDY: There are about 15 states--

- SEN. OWENS: Any of the surrounding states? Any--New York or Massachusetts, anything like that?
- MS. SMIDDY: New York has it under consideration. Massachusetts, I believe, has just recently--
- SEN. OWENS: Passed something?
- MS. SMIDDY: Passed a Bill. Rhode Island has. The earliest states, of course, were Florida and California. The western states, Idaho, New Mexico--
- SEN. OWENS: Has California had any test on their statutes in their Supreme Court?
- MS. SMIDDY: Not that I am aware of.
- SEN. OWENS: So, is there any case law decision on these various statutes, upholding--with respect to the constitutionality or problems that they're faced with on that at all?
- MS. SMIDDY: I do not know of any cases.
- SEN. OWENS: Okay. Representative Samowitz have a question? And then I want to go to Representative Chase who has a question.
- REP. SAMOWITZ: During the course of your panel discussion, one of the speakers I think mentioned the fact that somebody might be using an Apple computer to tie into an IBM computer and therefore somehow get some sort of benefit by getting to use the system. Is the crime that you want us to prevent the information obtained from that or the fact that somebody is using a lesser computer to go into an updated or higher computer?
- MS. SMIDDY: In many aspects, these are informational crimes. What we are concerned with--
- SEN. OWENS: Many are what? I missed that. I'm sorry.
- MS. SMIDDY: In many aspects, these are informational crimes that we are concerned with. The theft, misuse,

MS. SMIDDY: (continued)

unauthorized disclosure of information, but we are also concerned with people who act up a computer system and who disrupt its services to cause degradation of the services or who prevent authorized users from themselves using the system. So it's--

REP. SAMOWITZ: I mean is this the same type of situation where somebody who said they had a video player in his home and is using a television set to pick up an unauthorized transmission of a ballgame; is that the same type of thing? Or somebody that's using their own--somebody else's information for their benefit without really doing harm by doing that type of thing?

MS. SMIDDY: Well, some of this information, we must understand, is also highly confidential and very private information about people and we're not only concerned with people looking at that information, but someone who gets on a computer without permission, can inadvertently destroy the information or alter the information that is there.

You may recall the access to the Sloan-Kettering computer system where in fact, medical records were altered through inadvertence.

REP. SAMOWITZ: I can understand--we can deal with the various different ways and logical approaches to this problem and one is whether you're dealing with confidential information or public information. I mean there's all different types of information and the point that I'm trying to drive at is we don't want to hamper technological developments either. I mean, when one person uses one system and can somehow improve the technology by going to another system, we don't want to tie their hands down. We're not trying to be copywriters.

MS. SMIDDY: Oh, we're only talking about unauthorized use, where someone is using a system without permission of the rightful owner.

REP. SAMOWITZ: Well, I heard that within the hardware itself there was something said about an Apple computer being used for an IBM and in the hardware--not the software, but

18
klu

JUDICIARY

December 5, 1983

REP. SAMOWITZ: (continued)
the hardware system.

MS. SMIDDY: We could be talking, in that context, of a company that has established what we call a computer network where a lot of little computers are connected over communication lines to a large computer and I think that was the context that they were talking about.

MR. JOHNSTON: We are concerned with the fact that someone with a small computer can gain access to a large computer unauthorized. Now, there may be nothing more than utilize that computer's time but they have greater capabilities and so therefore, are degrading that larger computer because it does not have as much service to provide to the other authorized user. It's a theft of resources when they're using the computer time that the other can't use.

REP. SAMOWITZ: That's a horse of a--that's completely different than the situation that is involving taking privileged information off the information because that's a different class in itself.

MR. POST: We really were trying to--and it's broken down into several different kinds of crimes. One is--one area is when you, in an unauthorized way, enter somebody else's computer and look at the data, don't destroy it, don't take it, don't steal it, don't use it, merely enter in an unauthorized way, somebody's computer.

The second kind of crime is when you steal something from that computer in the sense that you're using the data, you're using the software programs; you're using a big computer for your own personal advantage without the authority to do so. You're in fact, stealing the owner's property rights to his own computer, whether it's General Electric or some of the big. A third area is when you destroy, whether it's destroying a software program, whether it's destroying data by entering a program onto a computer that methodically destroys all the data on that computer or whether it destroys the physical computer itself. And what we've tried to do is, and you will see it in the draft before you, all of those different kinds

MR. POST: (continued)

MS 2 of crimes, define them so that the layman can understand what it means when we're talking about access to computers or unauthorized use of the computer or informational data or entering a system, to define those terms and then begin to come up with the mechanics of how to deal with those.

REP. SAMOWITZ: I understand what you're saying. I can appreciate your concerns but I don't know if it's the same class, if you're talking about somebody who goes in to a smaller Apple computer and he is able to go and take the advantage of the--by linking into the wider data base of the memory storage capacity of a larger computer or is that the type of thing that you also want to regulate?

MR. POST: Well, one of the problems, if you have a little Apple or a little IBM or a little anything and you, in an unauthorized way, happen to enter Aetna's computer, through the telephone line, you may be able to gain information, change the rates for the policy issued on your life, change the data file on you as client of Aetna to eliminate--all through your little, small computer that sits--

REP. SAMOWITZ: Maybe this can drive what I want--what happens if Aetna says I have no problem with you people doing that? The computer hardware people who manufacture it say we don't want that to happen. Is that what this is involving?

MS. SMIDDY: No. The authorized user or owner of the computer is the person for whose benefit those services are provided.

UNIDENTIFIED SPEAKER: (not using mike.)

SEN. OWENS: Vin? Representative Chase.

REP. CHASE: Yes. This is addressed to anyone. Maybe Rusty would like to answer. I'm curious to know how many people or how many people have been convicted or charged with computer theft, destruction or anything of that nature? Do you have any figures on that, in Connecticut? And secondly, have they been convicted?

20
klc

JUDICIARY

December 5, 1983

REP. CHASE: (continued)

And thirdly, my third question is if they're convicted under current statutes, why do we need this? And the fourth question is why do we need this?

MR. POST: Really, the first question is it has to deal with the gap in Connecticut's law and the problem is some of the definitions that we now have in Connecticut law and how we define crime. It's the old description of what is proper and they don't always apply and the data software, and the misuse of some of these software programs is very hard under current Connecticut law to prosecute successfully a person who, in an unauthorized way, enters a computer, looks around and perhaps misuses some of that data.

Secondly, there's a problem of transmission of data. Our laws tend to assume that, for example, eavesdropping, we're talking about conversations which imply human to human and our laws tend to assume that the elements of a computer system is connected by a wire. They may not be. They may be connected by satellite, etc. So they need to revise Connecticut's laws to reflect the current state of technology and to deal with them. The trouble with these problems is what constitutes access to a computer and our laws just don't address those questions.

REP. CHASE: And so therefore, no one has ever been charged in Connecticut with computer thefts because you don't have the laws or--

MS. LOALBO: I'm not so sure that that's true. I'm not sure if anyone has been prosecuted specifically for crimes dealing with computer theft in Connecticut and I can tell you of phone calls that we received at CBIA and we have gotten phone calls complaining of this particular situation and they will say, our attorneys say that we can't prosecute this because--it doesn't constitute theft, or it wasn't an eavesdrop under the wiretap statute so they're saying that they're getting away with it because they're telling them that it's not possible for them to prosecute until--

MS. SMIDDY: Also, under the current laws, even when some sort

MS. SMIDDY: (continued)

of prosecution may be possible, it may not be realistic in terms of the situation. Someone may, for example, damage a \$20 tape volume and obtain \$45,000 worth of information. The criminal mischief statute would have us evaluate. The seriousness of the crime would be determined by the \$20--the value of the \$20 tape value instead of the more expensive information and therefore, there would be no reason for them to--

REP. TULISANO: Austin McQuigan will be here testifying in regard to the prosecution under criminal law if the questions come up. Vinnie?

REP. CHASE: Yes. Since the computer field is such a high tech field and it's constantly changing and new equipment, new ideas are coming out of the industry all of the time is this proposal that you make sufficient to address the changes in technology?

MS. SMIDDY: We tried very hard to make it so. We have both users and vendors, computer vendors represented on the committee and I can assure you that we have labored long over each of the definitions. For example, the definition of computer, we originally had the word digital in there and took it out simply because we felt that that might be too restrictive in terms of not only where the art is today, but where it's likely to go in the future. Yes, we paid a great deal of attention to that. We are very aware of the rapid expansion and growth and the change in technology as is characteristic in the computer industry and we don't want to have a law that reflects the current and past technology and would not cover the future.

REP. CHASE: Thank you.

REP. TULISANO: Representative Baronian.

REP. BARONIAN: Yes. I was wondering, before we get into more laws, certainly to try to protect the industry, what is the industry itself, the computer industry, high tech industry, doing to develop some kind of a system that might better prevent abuse of this kind? Are they or is it not possible?

MS. SMIDDY: There are currently both software and hardware, software packages and hardware devices where they have been designed to try to prevent abuse but it is impossible when you're dealing with people who are extremely sophisticated to eliminate it entirely and the risk of abuse is so substantial.

MR. POST: We had a fellow from IBM who was on the committee--he isn't with us today - but we met with him one day when he was describing it to us, they had a group at IBM whose only task was to break down the IBM computer system. As soon as they'd break down the latest IBM security system, they'd come up with a new way of changing security and that little task force goes to work in breaking that one down and it's a continuing process of the companies trying to develop a program, software program or hardware systems to prevent unauthorized access.

At the other end of the spectrum, we have a lot of small users who may not or could not afford a complex security system and it may be a simple thing like a customer list at the drugstore or the local insurance agency or what have you. Our laws don't yet cover the fact that if a competitor wants to foul up that computer user, they can destroy that data or change that data in a way that will put that person out of business.

MR. JOHNSTON: There's another important fact here and we've just discussed the fact that it's a high tech industry and it is advancing so rapidly that often commercial solutions are not economically preparable for a product that is going to be gone in five years. In fact, somebody designed it to make it available for the marketplace and that equipment is already passe and it's a limited market for sale and so the result is that a lot of the products are never going to see commercial solutions and there are a lot of businesses that capitalize and are pouring money into this equipment and will make long use out of, long beyond it's technological ability, they will continue to use it because it's economical for them.

REP. TULISANO: Senator?

SEN. DORR: It seems to me that--Senator Dorr--it seems to me

23
klu

JUDICIARY

December 5, 1983

SEN. DORR: (continued)
that I've heard testimony that in fact some people have perpetrated crimes already; is that correct? Crimes have been perpetrated in fact, one astronomical figure which has been skewed by statistics--

MR. JOHNSTON: That figure--I said \$450 million. It should have been \$450,000.

SEN. DORR: \$450,000 okay. Probably that bank robber in Los Angeles probably was the bulk of that, but nevertheless, these things are already illegal? I mean these people have been prosecuted? Is that correct? Is that an affirmative?

Some have? Okay.

MR. POST: Some have. When you talk to Dick Blumenthal who is not here today or Austin, you will discover from the Prosecutor's point of view that they have a hard time prosecuting some of these cases--

SEN. DORR: I see. Okay.

REP. TULISANO: They will never say they're not illegal. It's already illegal.

SEN. DORR: Okay, so what you're coming up here asking this Judiciary Committee to do is to pass further laws just to make it more specific as to what exactly is illegal; is that correct?

MS. SMIDDY: To clarify it and also to make sure that there are remedies available, appropriate to the harm. I was mentioning earlier the \$20 tape volume that gets stolen with \$25,000 worth of information on it. It's very possible that, although that may be illegal, the remedy is not in proportion to the harm that's been done.

I just want to, if I could, just speak--back up a little bit to the question about security systems, if I may. A lot of our conversations here have been focusing on unauthorized access by someone outside a company who is getting on to a computer system, but these computer crimes

MS. SMIDDY: (continued)

also occur as a result of people who are employees of a company and are, for some reason or other, wish to damage the company and one type of problem that occurs when-- and this has not been brought up here, is something called a time bomb program in which a disgruntled employee may, upon exiting a company, may leave within the system, undetected, a computer program which is "set" to go off at a given time or when a certain position occurs.

Now, this kind of program can effectively eliminate all the information that's in the system and then self-destruct, without leaving a trace and it may also simply cause other problems with the system which can occur at a later date.

If the person is already in the company and had access to the computer as an employee, the security systems wouldn't prevent that sort of thing from happening and this is in a sense, degradation and destruction of computer services which really aren't clearly defined.

SEN. DORR: I agree, although Mr. Post mentioned that the problems were with entry, the stealing of the information and the destruction so that would probably be the third type of computer crime. Just one last question, Mr. Chairman.

The testimony so far has indicated to me that no one has been prosecuted in the state of Connecticut and no one has been arrested; is that true?

Well, okay, Austin will tell us. Nevermind. Then, you are also seeking civil remedies as well; is that correct? So that you could go after these people civilly for destroying \$450 million or a lost week's work at GE or for whoever, whatever kind of rath the disgruntled employee or unauthorized access could cause? So you are also seeking civil remedies, as well?

MS. SMIDDY: That's correct.

REP. TULISANO: Are any of you concerned about the government getting into computers? Representative Berman.

REP. BERMAN: We're talking about seeking legal remedies, how easy is it to detect? I understand that it's easy to detect or that a crime has been committed, but how easy is it to pinpoint the perpetrator of the crime?

MR. MAGUIRE: Many, many of the computer crime cases that are reported, the person or the perpetrator would have gone undetected except for the fact that somebody squealed on them, because the lady who walked through the computer room with a magnet, that was probably something that we won't be seeing right away, but most of the crimes go undetected except when someone literally squeals on another perpetrator and then once somebody has a lead, being able to whack that.

I could give you an example of a case like that and I won't name the company, but the one that I'm familiar with, where two programmerd were hacking after they did their day's work as computer programmers, they would fool with the system and they have space and in that space and you can depict it like a record player and a piece of that disc was their space, historically, and they have unfinished official jobs and they work for their company there and they have the games and they have their own bookings and so you say here, I'm finished and they play their dungeons and dragons and whatever else they were playing with.

One of them has stolen the game from his compatriot and his compatriot found out about it so the compatriot buries a time bomb in his friend's disc so that it exploded and erased everything on it, including the company's work that he had in various unfinished states and when his friend discovered that and he suspected who it was, he reported it to his supervisor and that's where the company got knowledge of it and the acvities that both of them were doing and doing improperly. But for that particular way of one employee getting back at another, the company would have been (inaudible) And that's very often how these things are discovered.

REP. BERMAN: So that actually anybody who has obtained access to another computer system can go--literally can go undetected unless somebody turns them in?

- MR. POST: You can trace, though, can't you Brian? You were describing that a company can put a tracer to see what you're doing with your terminal and find out what--
- MR. MAGUIRE: It depends on the technology. If you use the long distance telephone lines, there's usually a way to work out a solution with that and you can get a record of the telephone call and that can be traced to a kind of electroid--some kind of electronic line that they have in the system, but very often, it is not traceable unless--
- MS. SMIDDY: Sometimes also, companies will just simply automatically just take a survey of who's on the system and what they're doing and if anything looks amiss or there are things called accounting routines that reveal that there are either jobs or whatever--that something looks wrong and people can be detected that way also.
- REP. BERMAN: In other words, we can design legislation that would be--that would cover all aspects of computer crime as you know it now, but the detection and the apprehension would be unlikely, is that--
- MS. SMIDDY: Oh no. I don't think so. I think as an example of the detection, we have very good examples in the much publicized hacker case where the FBI was able to once they were alerted to someone who was tampering and the arsonist or other systems--they were able to determine who was there and to trace calls.
- MR. JOHNSTON: If I may, detectors, as far as in computers, is not much different from shoplifters in a retail store. The more protection that you put out, cameras, surveillance and what have you, the more you're going to detect the shoplifter before they get out of the store. The only way you know beforehand is
It's the same way with the computer. You know that it's been happening and you put in more protections and you trap and catch.
- REP. TULISANO: Representative Rybak.
- REP. RYBAK: Mike Rybak, 66th District. I have two drafts

REP. RYBAK: (continued)
before me. I have your committee draft, dated 12-1-83, and I also have the Judiciary Committee's LCO 27 and I'm trying to compare both of them to arrive at a conclusion as to what the legislation may look like.

My first question concerns fraudulent use of an automated teller machine, ATM, obviously that fits the definition of a computer taking money from the machine which would be misappropriation of property. Would this be an offense in addition to the law which we passed last year for fraudulent use of an automatic teller machine?

MS. SMIDDY: One of the concerns of the committee is to evaluate our proposed draft and in conjunction with current legislation and to eliminate overlap. I will quite frankly state we haven't gotten to that point in the legislation. I know that we are depending, for example, on the larceny, the traditional larceny statute, to take care of some aspects of the computer crime and my sense is that based on the committee's past activity that when there is currently legislation, Connecticut legislation which covers the situation, you will rely on that legislation to continue in covering the situation rather than have duplication. You will, in our proposed draft, I'm sure find that there are examples of situations where there may be duplication simply because we have not worked through this draft.

This is still a draft and it's at the stage where we have gone through the definitions and we are working our way through the definitions of the substantive crimes.

REP. TULISANO: I might just add for the Committee's information, that there will be other drafts I'm sure, available which will be available to the Committee for future discussion which will attempt to--the Co-chairs are working with this committee to try to develop something and submit it to everybody. We will start kicking around those answers I think in January or before we get into session.

REP. RYBAK: In the computer crime committee's draft, page 3, bottom of the page, classification of computer related crimes, carried over on the next page it says that any

28
klu

JUDICIARY

December 5, 1983

REP. RYBAK: (continued)

person who conspires to commit, attempts to commit or causes another to commit any offense within this part, shall be punished as though he had committed a crime. Do you mean to say that it will be a crime and a specified felony or misdemeanor?

MS. SMIDDY: To the same extent that--as if he had committed -- some principal who had committed the crime. A lot of that language was picked up from the current Connecticut statute dealing with attempt and conspiracy.

Perhaps I should tell you that we have, our committee has worked through the statute down through page 2 section b and we presented this draft to let you know that we have a statute that is structured to cover the major areas of computer crime and that we do intend to be able to complete it by January. This really was for informational purposes at this point.

REP. RYBAK: Okay, my only concern was, and I didn't realize that was the current law, the phraseology as though someone had committed a crime. The only way I know to punish someone is in fact if they have committed a crime.

MS. SMIDDY: Yes, I think your point is well taken.

REP. RYBAK: With respect to cites of the crime, the concept that's in your draft and it's not in the Judiciary Committee's draft is that if any part of the computer system is located in the state of Connecticut, even though the caller may be outside the state or the accessor may be outside the state, there's sufficient jurisdictional anaxis with which to prosecute. Are you satisfied that that is in fact, sufficient jurisdictional anaxis?

MS. SMIDDY: That is also an area that we have yet discussed. What we did in drafting the Bill was to draft a Bill that covered the major areas or the major concerns of the Committee as they identified them and we have been working through each section. We have not, as I said, gotten past the middle of page 2, to determine whether in fact, that is supported--whether it conflicts with other Connecticut law or satisfies the jurisdictional requirements.

REP. RYBAK: My only comment on that would be I would suspect that some of the lesser offenses would be misdemeanors since you generally cannot extradict for misdemeanor, you'll never get the person in the jurisdiction to prosecute.

I don't mean to pick this apart. I'm just trying to work at some of the concepts here that are in the two drafts.

The question of intent with respect to unauthorized access seems to become the most difficult question. Obviously, you not only have to have the act, you have to have mens re or the intent to commit the time itself. How would one go about proving intent to commit a crime where there simply was unauthorized access as one of-- I think both bills define that as an offense, where there was no misappropriation of property or invasion of privacy of that sort?

MS. SMIDDY: There are several ways. One is a hacker or other person could simply use a random number generator to try to dial the computer. Another one is they could use some sort of a computer program or some sort of--to determine what the password is if they do not in fact know what the password is.

Those are the two indicia what someone who is not authorized would do and would be very easy to prove.

REP. RYBAK: Would that be sufficient to distinguish it from the case of the 14 or 15 year old genius who, fooling around with his home computer accidentally accesses somebody's main frame?

REP. TULISANO: This is still blank, is what we call it on this draft. You might explain why.

MS. SMIDDY: This has been an area of major concern to the committee and one that we have devoted a lot of time to. We have not arrived at a satisfactory resolution of how we want the language in that section defined and that's why it's blank in the section, but it just seem just and simply in talking about proof, that if one can

MS. SMIDDY: (continued)

establish that one uses one of those methods that I was just talking about, and stays on the computer, then that would be the factual establishment of an intent to make an unauthorized access. A person who is authorized is not going to need to use a random number generator to dial up a computer or--nor will the person need to get the password by trial and error.

SEN. DORR: So in effect, you've created a crime of computer trespass, basically? That's what you're working on? Which is very difficult to prove intent.

REP. TULISANO: It's probably squatting rights. When we were talking about this little piece of area, when you hold it up, that's in a way, squatter's rights. That's squatting and trespassing. Don't laugh. We have common law minds. Representative Dorr.

SEN. DORR: One final question. With respect to the Judiciary Committee's draft, there is a treble damage civil remedy for anyone whose personnel files or insurance files have been accessed and some way information taken for an improper purpose or by an improper party. Would you foresee the eventual creation of the statute to include some form of private cause of action to protect the individual?

MS. SMIDDY: Absolutely.

SEN. DORR: As well as the large company?

MS. SMIDDY: Absolutely. That is an area that we are extremely concerned about. The privacy issue cannot be underestimated here, nor can the issue of access to personal records which will cause some physical harm to the person such as medical records. We have--I'll give you an example of medical records being altered at Sloan-Kettering and the potential problems that this can cause can't be underestimated. Also, as you know, computers are also used now in medical diagnosis and to administer anesthesia, etc., and interference with computers which may potentially cause a health problem are another area of concern.

MR. POST: I think that another aspect of that is in addition in criminal proceedings that we're discussing in the committee we have devoted almost an equal amount of time maybe more to civil remedies which may in many instances may be better in dealing with the situation trying to persuade a prosecutor. So the draft that you will eventually get will also include not only our suggestions as to what constitutes a crime, but also our suggestions as to some civil remedies as well.

REP. RYBACK: Given the difficulty of detection and the challenge of some of these crimes -- the perpetrators do you feel the statute would be a deterrent or simply a remedial measure.

MR. POST: It depends on -- the criminal may turn out to be more of a deterrent. If you can turn to the 15,000 people that crime is referred to with access to the computer and make it clear to them that going into unauthorized areas is a crime, that may slow down some people who otherwise may think it was funny, a time to play games. But the civil remedies may be a very effective deterrent. If somebody faces troubled damages, the attorney's fee etc., because they didn't use or steal data from your computer, or tried to take your customer list or what have you, that may be both remedial and very much deterrent. I hope it would be both.

SEN. DORR: Thank you.

REP. DORR: Thank you. Any questions from this panel? Thank you ladies and gentlemen. Do you have anything else you want to add? Wait until you see the next two we're going to put up together. Austin McQuigan and Bill Olds. This is a first in history. While we're waiting - (inaudible)

AUSTIN MC QUIGAN: I would ask the Chairman to note that Mr. Olds is sitting to my right. I don't know what significance we can attach to that.

: As we look at it Mr. McQuigan, he's sitting to your left.

MR. MC QUIGAN: We have been working on a draft in our office we have some copies for you. Outside of that short statement

MR. MC QUIGAN: (continued)

which I won't bother to read, we have attempted to put some language down, what we would call criminal trespass to a computer system and that's really what we feel is a major area of concern. There are three areas, one is larceny, using a computer that's covered by the present criminal statutes fairly well. Larceny of information we might need to -- computer information, we might need to clarify, and the second area would be mischief where someone accesses into a computer system and destroys some or all of it or disrupts it electronically or otherwise, we might need to clarify the criminal mischief statutes. We've been working with the AdHoc Committee and Rep. Tulisano and Sen. Owens trying to draw some language there.

And finally, is there area of trespass which is complicated we feel by the fact that there are many computer systems which are at present open to the public for the public use and we cannot simply issue a legislative fiat to block access totally. So we have tried to craft some language which on the one hand will forbid accessing a system that you're not authorized to access and at the same time will not completely restrict the flow of information. I think that Bill and I have had the same concerns here and I think he's also concerned with providing some protection for privacy, but also getting a statute that we can live with.

MR. WILLIAM OLDS: I think the key point here is that Austin and I are in agreement that --

MR. MC QUIGAN: This is an historic moment.

MR. OLDS: I think we both place a different emphasis as you heard from the previous speakers which we're in essential agreement on, we place a stronger oneous on the owners or the managers of those computers whether they be in government or private industry. I think this Committee is really on the threshold of something extremely important. It's a very complicated subject, but the legislature over the years has been very sensitive, I believe to the whole issue of individual privacy. I think 76 and 77 that the legislature passed a personal data act which relates to state and computerized data which

MR. OLDS: (continued)

gives citizens access to state agencies. Last year the Connecticut Insurance Information and Privacy Act which applies to insurance companies went into effect that gives you and I access to data about our insurance records. I have a long three page statement which I will not read and which I will read with the committee, but I'd like to hit the highlights of it and maybe the three of us can see.

The previous speakers from private industries acknowledged that it's very difficult to detect unauthorized entry into computers. I think that we must be very careful that we do not become solely preoccupied with teenage hackers who gain access to our files like erasing records or rearranging the files or even peeking into personal records. They do a great deal of damage and we do need to deal with that aspect of it as has already been recommended.

But the computer managers who let them inside those systems I think are also . If I loan my car to a business associate, and that individual leaves that car with the keys in it and the doors unlocked, I think I should have a cause of action against that individual. In the same way, if I provide information to the government or private industry, they have a responsibility to maintain reasonable security measures so that my right to privacy is not violated. I'm not an expert in the area of computer technology, but I have read extensively on this subject and I believe that there are reasonable -- that technology has reached the state where there are reasonable security measures that can be established.

There will be reasonable differences of opinion among some of the people in this room as to whether the technology then jumps ahead of its security measures and that from time to time may be a problem. But the point is that some security measures do exist and I think that the managers of those system or owners of those systems have a responsibility to establish strong security provisions. I have five or six specific recommendations. Some of them you may not want to consider for this specific bill, but you may want to consider separate legislation. Number one, I believe that Connecticut should pass legislation

MR. OLDS: (continued)

applicable to both government and industry which incorporates the principle that there are proper approaches to the management of information of that agency or industry to take conservative steps to ensure that their information management practices conform to a reasonable set of norms. That language already exists in a federal privacy act. The federal law essentially says what I just stated. Let me read to you the key elements of the federal privacy act. The problem is that that applies only to federal agencies, not state agencies.

The federal privacy act says, "may show established appropriated administrative technical and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security." and it goes on from there. I think language similiar to the privacy act must be considered here. Number two, we support the thrust of the bill and there may be some differences to the language but nobody can argue that getting into a computer without authority is significantly different than a kid who breaks and enters the building and screws up the system in some manner. Number three, the personal data act which was passed by this legislature in 1976 applies to state agencies.

I think it should be amended to apply to municipal government which often operates their own data processing systems. At the present time the state law provides privacy protection to individauls, it gives you and I access -- limited access to state agencies, but not to any other government body. Four, the personal data act, called the privacy act in Connecticut should also be amended, I think, to incorporate the security principles I quoted earlier that are part of the federal privacy act. The present state law, I don't think adeqatly addresses the security issue.

Number five, the Civil Liberties Union position about the individual's right to inspect his or her own file is certainly something that should be considered. That to a significant degree is already in existance in terms of access to state agencies. But its always been our position that each person should have the right to inspect any information about him or herself and be able to correct or

MR. OLDS: (continued)

contest that information. And finally, Connecticut, I think, should consider adopting language similar to the law passed by the New York General Assembly this year which is called the personal privacy protection law. That law is somewhat unique in terms of privacy because they have something in New York State called the Committee on Open Government and that -- under the new legislation passed a couple of months ago, that committee can review all new or modified record systems before they are instituted.

This exposes to public scrutiny every governmental decision to accumulate and use personal information in New York State. I think Connecticut should give serious consideration to the establishment of a regulatory agency to deal with the growing threat to privacy by data banks. Thank you.

MR. MC QUIGAN: Well I'm not adopting all of Bill's recommendations but I think the committee bill left open the question of trespass in its draft because of concerns over how to word it. I think you should consider the question, not only when Bill talks about an affirmative duty on the part of industry to protect the information, the cost factor that we're dealing with here for small business, that also you just can't jump into that position. And what we tried to do is try to go down a middle ground here. Our proposal what it does is it deals with a person accessing without authorization.

But then in effect, what we do is we say it's an affirmative defense to a prosecution that the believes that the owner did license him or would license him to go in or that he recently could have not known that his access was unauthorized. It's difficult to draw, I think, an affirmative duty on the part of business to provide protection because of the cost factor and that should be -- on major industry that may not be a significant problem and I suspect they certainly do that at the present time. But for the small pharmacy, that type of business, supply store, they might be in a very difficult position to try to modify their system. So I think it's an area that's complicated and one would want to go slowly and work on it.

REP. TULISANO: In your draft you have a person guilty of criminal

- REP. TULISANO: (continued)
access it says when knowing he is not authorized to do so. Then use an affirmative defense, if they have reason to believe that the owner of the computer system allowed him to do that, if he knows he's not authorized why are you using the --
- MR. MC QUIGAN: That appears to be duplicative, but it was done intentionally in the sense that we are trying to -- we are wrestling whether or not, as you point out to me it should be an affirmative defense or the state would have to prove it. Beyond a reasonable doubt.

And that is obviously what we're addressing and we're throwing it out that way for discussion purposes. Because that -- if we have the burden, we simply may not be able to make that burden. And I'm not sure how we should go on that, but we did discuss that on Wednesday.

REP. TULISANO: Do we have a choice.

MR. MC QUIGAN: I feel that an affirmative defense is the best method to go and I'm sure Bill disagrees with that.

REP. TULISANO: Is it generally allowed.

MR. MC QUIGAN: Pardon?

REP. TULISANO: Is it generally allowed in affirmative offenses?

MR. MC QUIGAN: In a trespassing a good analogy to what we have here is the trespass law. What you're really talking about is trespassing into a computer system and now what we're saying -- Bill's saying is you should be required to put a sign up, "No Trespassing". And I'm saying that may be too expensive in certain cases. So the question is how do you give people the opportunity to go into buildings or computer systems that are public and at the same time deny them when we want them confidential. One is put up signs that may not always be possible.

The other is to say that under circumstances where a reasonable person would have known they didn't have authority then in fact we can prosecute the case. And to make that an affirmative defense. Certainly it would enhance the

MR. MC OUIGAN: (continued)

prosecution of the case if you had a sign up. But to bar a prosecution without a sign may deprive any protection for a number of unsophisticated computer systems. Certainly the sign would be an electronic sign of some sort when you went in saying "you're not authorized for this information." An analogy to the trespass law and the trespass law does use an affirmative defense for a class B misdemeanor. Whether that's workable or not, that's something we should carefully debate.

But I think it's an important area. Protecting people's privacy and providing criminal protection is important. In the larceny area we have simply not had the criminal experience to warrant a belief that at this time it's significant. It's simply we have not had the cases in Connecticut. It's estimated to be a \$100 million a year problem which is not a significant criminal problem when one looks at the white collar crime in the United States which is estimated at \$50 billion. So that we have put a budget proposal as usual for the last three years we have made budget proposals for a computer crime unit along with things like an Inspector General's Office and various other things. We know that will be greeted warmly, but I would suggest that if we are going to pass a substantive law in this area, that's going to have some meaning, we're going to have to have an investigator who understands this area.

We're going to have to have expertise or else it's going to be a substantive law with now enforcement capacity and will fall into this and not be enforced and that's real. If we're going to pass the law we're going to have to hire somebody to handle these cases who has the experience with computers so he or she can put the case together in an orderly way. It's an area far beyond what we have in investigative prosecutive capacity right now. With all due respect the Girard Federal Case really simply is a larceny case of computer information and it's taking information off of a computer, confidential drug enforcement and selling it and it was done by selling the information to the undercover. And it really doesn't -- it's not the type of electronic snooper that we're talking about and getting into.

MR. MC QUIGAN: (continued)

So if we're going to do the cases we're going to have to have some money as usual.

REP. TULISANO: Bill, do you think the federal damage kind of area is something that we should be getting into in terms of civil liberty suits?

MR. OLDS: Yeah, I do think that, as the industrial representative suggested also that might serve as somewhat of a deterrent to some of the hackers or whatever you want to call them. I think it serves as a deterrent. I'm skeptical though that the reality is that most people who gain access are not going to be detected. And I'd like to see placed a stronger emphasis on the other end of it. The responsibility to the owners.

REP. TULISANO: My feeling is that you're talking about the government to some extent. Do you find government abuse of its -- you're talking about the municipal government, do you find that exists in Connecticut?

MR. OLDS: Yeah, abuse of its record keeping. There have been examples, I believe in Norwalk or Orange, Connecticut, there have been abuses. And there have been some Congressional studies done during the last two years including one I think that was incorporated in the federal privacy report which showed that government agencies have on a number of occasions collected information that they were not supposed to collect, released information that they were not supposed to release.

REP. TULISANO: Thank you. Any member from the public that has signed up. Is there anybody in the audience as members of the public that would desire to address the committee at this point in time. Seeing none, we'll call this public hearing to a close. Thank you very much ladies and gentlemen.