MEMORANDUM

TO: Carl Pabst

FROM: Stephen Plafker

SUBJECT: Comparison of Present Section 502 with Comprehensive Computer Data and Fraud Act

DATE: December 8, 1986

The following is a comparison of the present Penal Code Section 502 with the Act. Comparible portions are placed next to each other. Portions in one but not in the other are underlined.

1. Definitions

Access.
- Present Section. to instruct, communicate with, store data in, or retrieve data from, a computer system or computer network
- Proposed Section. to gain entry to, instruct, or communicate with the logical, arithmetical or memory function resources of a computer, computer systems [sic], or computer network

Computer Network
- Present Section. an interconnection of two or more computer systems
- Proposed Section. two or more computer systems connected by telecommunication facilities

Computer Program [software]
- Present Section. an ordered set of instructions or statements, and related data that, when automatically executed in actual or modified form in a computer system, causes it to perform specified functions
- Proposed Section. a set of instructions or statements, and related data that, when executed, cause the computer, computer system, or computer network to perform specified functions

[Computer] Services
- Present Section. includes, but is not limited to, the use of the computer system, computer network, computer programs, or data prepared for computer use, or data contained within a computer system, or data contained within a computer network
- Proposed Section. includes, but is not limited to, computer time, data processing, or storage functions, or other uses of a computer, computer system, or computer network

Computer System

Present Section. a device or collection of devices, excluding pocket calculators which are not programmable and capable of being used in conjunction with external files, one or more of which contain computer programs and data, that performs functions, including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control

Proposed Section. a device or collection of devices, including support devices and excluding pocket calculators which are not programmable and capable of being used in conjunction with external files, one or more of which contain computer programs, electronic instructions, input data, and output data, that performs functions, including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control

Data

Present Section. a representation of information, knowledge, facts, concepts, or instructions, which are being prepared or have been prepared, in a formalized manner, and are intended for use in a computer system or computer network

Proposed Section. a representation of information, knowledge, facts, concepts, computer software, computer programs or instructions. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device.

Financial Instrument

Present Section. includes, but is not limited to, any check, draft, warrant, money order, note, certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction authorization mechanism, marketable security, or any computer system representation thereof

Proposed Section. not defined

Property

Present Section. includes, but is not limited to, financial instruments, data, computer programs, documents associated with computer systems and computer programs, or copies thereof, whether tangible or intangible, including both human and computer system readable data, and data while in transit

Proposed Section. not defined

['The words "personal property" include money, goods, chattels, things in action, and evidences of debt;...' Penal Code Section 7(12).]

Supporting Documentation

Present Section. no definition

Proposed Section. includes, but is not limited to, all information, in any form, pertaining to the design, construction, classification, implementation, use, or modification of a computer, computer system, computer network, computer program, or computer

software, which information is not generally available to the public and is necessary for the operation of a computer, computer system, computer network, computer program, or computer software

Injury

Present Section. any alteration, deletion, damage, or destruction of a computer system, computer network, computer program, or data caused by the access, or any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was not altered, deleted, damaged, or destroyed by the access

Proposed Section. any alteration, deletion, damage, or destruction of a computer system, computer network, computer program, or data caused by the access, or any expenditure reasonablly and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, deleted, damaged, or destroyed by the access

2. Provisions

Fraudulent Access

Present Section. Any person who intentionally accesses or causes to be accessed any computer system or computer network for the purpose of

(1) devising or executing any scheme or artifice to defraud or extort, or

(2) obtaining money, property, or services with false or fraudulent intent, representations, or promises ...

Proposed Section. Knowingly and without permission accesses and alters, damages, destroys, or otherwise uses any data, computer, computer system, or computer network to devise or execute any scheme or artifice to defraud or deceive or control or obtain money, property, or services by means of false or fraudulent pretenses, representations, or promises. Subsection (c)(1)

Malicious Access

Present Section. Any person who maliciously accesses, alters, deletes, damages, destroys or disrupts the operation of any computer system, computer network, computer program, or data ... [Definition of "malicious". "a wish to vex, annoy, or injure another person or an intent to do a wrongful act, ..." Penal Code Section 7(4)]

Proposed Section. not explicitly in the proposed bill but I believe it is covered in the following: 1. Knowingly and without permission accesses and adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network. Subsection (c)(4). 2. Knowingly and without permission accesses and disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an

authorized user of a computer, computer system, or computer network. Subsection (c)(5)

Illegal Access

Present Section. Any person who intentionally and without authorization accesses any computer system, computer network, computer program, or data, with knowledge that the access was not authorized ...

Proposed Section. Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network

3. Other Provisions of Proposal

Theft of data. Knowingly and without permission accesses and takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network. Subsection (c)(2)

Theft of services. Knowingly and without permission uses or causes to be used computer services. Subsection (c)(3)

Assistance. Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network. Subsection (c)(6)

BILL ANALYSIS

AG/D Office

BILL NO. SB 255
AUTHOR Senator Davis
DATE LAST AMENDED

ANALYST R. R. Granucci
DATE February 27, 1987
TELEPHONE (415) 557-1959

I. SUMMARY OF EXISTING LAW

California's current computer crime statute, Penal Code section 502, sets forth in subd. (a) a series of definitions of computer systems, data, networks, etc. Subd. (b) prohibits the use of a computer system to devise or execute a scheme to devise or defraud, or to steal money or services. Subd. (c) makes it a crime to maliciously access, alter, disrupt, etc. any computer system, program or data (computer "vandalism"). Subd. (d) covers unauthorized access or "hacking."

Subds. (e) and (f) provide penalties. Violation of subd. (b) or (c) is alternatively punishable as a felony or a misdemeanor; a first violation of subd. (d) which does not cause injury is punishable as an infraction while a second violation or one that causes injury is punishable as a misdemeanor. Subd. (g) permits any victim to bring a civil action with provisions for parental liability and attorney's fees and subd. (h) disclaims any intent to preempt prosecution under other provisions of the criminal law.

Thus, section 502 in its current form does four things. It (1) defines terms, (2) declares conduct to be criminal, (3) specifies punishment and (4) provides for collateral civil remedies.

II. SUMMARY OF BILL

SB 255 totally repeals and then reenacts section 502. A savings clause is included to prevent the abatement of prosecutions under the present law.

The new section 502 follows the same general format as the current law; i.e., definitions, crimes, punishments and collateral remedies, but makes significant changes in each of these areas.

Definitions

The definitions in the new section are broader and directed more to computer users than to lawyers. Newly defined terms include "supporting documentation" and "injury."

Crimes

Subd. (c) of the new bill sets out seven species of crimes and reaches conduct that is not covered under present law. The crimes are (1) the access, alteration, destruction, etc. of a computer system, program, network or data to devise or execute a scheme to defraud, or to obtain wrongfully or control property or money by false pretenses; (2) taking or copying data; (3) unauthorized use of computer services; (4) accessing, altering, damaging, etc. data, software, programs or supporting documentation, in other words, vandalism; (5) disrupting or causing the denial of computer service to an authorized user; (6) providing or assisting in the providing of a means for unauthorized access; and (7) unauthorized access, or "hacking." This last provision is essentially a simple trespass law; in substance, it simply replicates current law.

SB 255 retains the provision in present law which provides a defense "to any person who accesses his or her employer's computer system [etc.] . . . when acting within the scope of his or her employment."

This provision in the present version of section 502 has not, to my knowledge, proven to be a source of difficulty for prosecutors. It is intended to exclude any employee whose good faith use of the employer's computer may be in technical violation of his job specifications. Examples might include an attorney who, without permission from the supervisor in his firm's word processing department, uses the equipment after normal working hours to prepare a pleading, or an employee who uses electronic mail to send a short personal message. In many instances, employers tacitly overlook such conduct either because they feel it's not worth bothering about or in the belief that employees' enhancement of their computer skills works to the employer's long-term benefit.

Significantly, the mental elements of "intentional" and "malicious" in the current section 502 are replaced with "knowingly" and "without authorization." Thus, the mental element under the new bill is general criminal intent, rather than malice. This single change will definitely make the statute easier for affected persons to understand as well as aiding its enforcement.

Punishment

Punishments generally remain the same as under current law; i.e., alternative felony or misdemeanor punishments are provided for most violations, the maximum felony punishments being 16 months, two or three years, the maximum fine being $10,000. A first violation of subd. (e)(3), theft of services, is punishable as a misdemeanor if no injury results and the value of the stolen services is less than $400. Repeat violations, or those which cause injury or involve more than $400 worth of service are alternatives punishable as felonies.

Collateral Remedies

The collateral remedy provisions of the present law are substantially reenacted. The attorney's fees provision in the present section 502(g) is changed from "prevailing plaintiff" to "prevailing party." A new provision permits computer equipment used in violation of the law to be seized and destroyed as contraband, or turned over to a public agency or nonprofit corporation as deemed appropriate by the court.

III. BACKGROUND INFORMATION

SB 255 is essentially a fine-tuned version of a bill authored by Senator Davis last year which narrowly failed to pass. That bill, SB 1786, was approved in principle by our office and was endorsed by the CDAA.

IV. RECOMMENDATION

Consistent with last year's position, we should approve SB 255 in principle.

APPROVED: John H. Sugiyama

John H. Sugiyama

BACKGROUND SHEET FOR THE SENATE JUDICIARY COMMITTEE
ON
SENATE BILL 255 (DAVIS)
LOS ANGELES COUNTY-SPONSORED

1. WHO PROPOSED THIS MEASURE?

Organization: Los Angeles County Phone: 441-7888

Name to Contact: M. Steven Zehner

2. WHY IS THERE A NEED FOR THIS BILL?

Background of Problem:

Under existing law, various criminal and civil sanctions are imposed for the unlawful use of computers and data systems. Private system operators and prosectuors believe enhanced penalties and further standardization of definitions are needed.

In 1984, an American Bar Association report on computer crime estimated the annual loss to industry ranges between $145 million and $730 million. This range is so broad because of the difficulty in pinpointing the specific impact of computer crime.

Computer crime is a major problem which becomes worse with each technological advance. The same improvements that make information systems more flexible and useful also facilitate illegitimate uses of computers and data systems.

California is a national leader in the area of information systems, and we should make an all-out effort to protect this important industry.

Description of Bill:

Senate Bill 255 (Davis) was developed by a task force composed of experts from both the private industry and the criminal justice community. The bill broadens the application of existing law by redefining such terms as "access," "computer system," "computer network," "computer program," and "data." Moreover, SB 255 would define new terms such as "computer services" and "supporting documentation."

Senate Bill 255 also provides for increased penalties for computer-related crimes such as fraud, data theft, tampering with systems and publishing access codes. These offenses, which are now misdemeanors, would become "wobblers," alternative felonies/misdemeanors.

Finally, SB 255 would provide for the forfeiture of materials and equipment used in the commission of this crime.

How would this bill help resolve this problem:

Enactment of SB 255 would provide for uniform standards and definitions of computers. It will help to protect a major industry in California as well as to give law enforcement the necessary tools to act against those who seek to generate illegal profits from information systems.

3. HAS THERE BEEN RELATED LEGISLATION INTRODUCED IN THIS OR PAST SESSIONS? IF SO, PLEASE LIST.

Senate Bill 1786 (Davis) was introduced during the 1985-86 Legislative Session.

Senate votes on SB 1786 were as follows:

Senate Judiciary:	6 ayes; 0 noes
Senate Appropriations:	Senate Rule 28.8
Senate Floor:	28 ayes; 1 noes

4. WHO SUPPORT OR OPPOSES THIS MEASURE?

Opposition: There is no known opposition to SB 255.

Support: California Chamber of Commerce, California Manufacturers Association, Equifax Corporation, Rockwell Industries, Hughes Aircraft, Northrop Corporation

SZ:DS1
SB255-WS