SENATE COMMITTEE ON JUDICIARY
Bill Lockyer, Chairman
1987-88 Regular Session

SB 255 (Davis)
As introduced
Penal Code
TDT

COMPUTER CRIME

HISTORY

Source: Los Angeles County Board of Supervisors

Prior Legislation: SB 1786 (1986) - Died in Assembly Judiciary
AB 2551 (1983) - Chaptered

Support: Union Bank, Security Pacific National Bank, Information Systems Security Association, Southern California Gas Company, California Bankers Association, Hughes Aircraft, Santa Cruz County Board of Supervisors, Northrop Corporation, Los Angeles County Sheriff, Attorney General, Equifax Inc., Los Angeles County District Attorney

Opposition: No known

KEY ISSUE

SHOULD A COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT BE ADOPTED WHICH WOULD REDEFINE A NUMBER OF COMPUTER TERMS, ESTABLISH SEVEN SPECIFIC CRIMES, PROVIDE FOR COMPENSATORY DAMAGES AS CIVIL REMEDIES AND PERMIT SEIZURE OF PRIVATE COMPUTER EQUIPMENT?

(More)

PURPOSE

Existing law makes it a crime, punishable by imprisonment and fines which in no case may exceed $10,000, for any person to, among other things, access a computer system or network: 1) intentionally in order to defraud or extort; 2) maliciously; or 3) intentionally and without authorization, with the knowledge that the access was unauthorized.

This bill would repeal and then rewrite Penal Code Section 502. It would broaden existing definitions, expand the scope of prohibited computer related activity, and restructure fines and imprisonment penalties for violations.

It would reenact civil remedy provisions and add a new penalty of seizure of computer equipment used in committing violations of the act. Finally, it would set forth the legislative intent of this bill.

The purpose of the bill is to clarify and broaden existing law, as well as provide increased penalties commensurate with the gravity of the offense.

COMMENT

1. Background

   This bill was developed by the Computer Crime Task Force, which is a subcommittee of the Los Angeles County Criminal Justice Coordinating Committee. The Task Force is composed of 16 members including representatives from law enforcement, district attorney offices, the

(More)

U.S. Attorney's office, and private industry, including banks, accounting firms and big business. No representatives of the defense bar are on the Task Force. The primary duty of the task force is to develop a Model Computer Crime Act; and, in so doing, it created a bill which it believes would meet the specific computer crime problems in California.

2. Standardization of definitions

This bill would broaden the application of existing law by redefining terms that are used in existing law, such as "access", "computer system", "computer network", "computer program" and "data". It would also define new terms, such as "computer services" and "supporting documentation".

The task force believes that it is necessary to provide standard definitions in order to insure higher conviction rates. Proponents believe that the new definitions would be broader, and would be directed more to computer users than lawyers but would be acceptable to both the business and legal communities.

3. New crimes

This bill would create seven new crimes involving computers. Any person who did any of the following acts, if the act was not within the course and scope of employment, would be guilty of a crime:

(More)

a) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud or deceive, or (B) wrongfully control or obtain money, property, data, or services.

b) Knowingly accesses and without permission 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.

c) Knowingly and without permission uses or causes to be used computer services.

d) Knowingly accesses and without permission 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.

e) Knowingly and without permission 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.

f) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or

(More)

computer network in violation of this section.

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

4. Penalties

Existing penalties for maliciously or intentionally accessing a computer system or network in order to defraud or extort is punishable by imprisonment and a fine which in no case may exceed $10,000. Intentionally accessing a computer system or network without authorization when no injury results, is an infraction punishable by a fine not exceeding $250. If injury results, or if it is a second offense, the fine could be imposed not to exceed $5,000 and/or imprisonment in county jail not exceeding one year.

This bill would increase the penalties as follows:

a. Access (Hacking)

1) A first offense or an offense where no injury occurs would remain an infraction punishable by a fine of up to $250.

2) Repeated access or access resulting in injury would be punishable as a wobbler, by a fine of $10,000 maximum or imprisonment in state prison for 16 months or 2 or 3 years or both, or a fine of $5,000 maximum or 1 year in county jail or both.

(More)

b. Unauthorized use of computer services

1) A first offense without injury where the value of services used is $400 or less, would be punishable by a fine of up to $5,000 or one year in county jail or both.

2) Subsequent offenses or violations causing injury would be subject to the same felony/misdemeanor punishment as repeat access or access with injury.

c. Remaining computer crimes

All the remaining computer crimes including altering, data theft, tampering with systems, publishing access codes, disrupting, or committing fraud or theft via computer, whether a first or subsequent offense, would be subject to the same felony/misdemeanor punishment as repeat access or access with injury.

5. Civil penalties

In addition to any other available civil remedies, the owner or lessee of the computer would be permitted to bring a civil action against any person convicted of any of the enumerated crimes for compensatory damages. Actions of an unemancipated minor would be imputed to the parent or legal guardian having control or custody of the minor. The court would be authorized to award reasonable attorney's fees to a prevailing party.

(More)

6. Intent not required

Under existing law, the criminal conduct must be "intentional" or "malicious". This bill would establish a new standard that the conduct be "knowingly and without permission". Proponents claim that this new standard would make these crimes "general intent" crimes, which would be easier for the public to understand and authorities to enforce.

One effect of this change would be to make such acts as unintentional and inadvertent alteration of data by an employee using a computer for a personal project without permission, subject to a state prison term.

7. Felony penalty for first time access

Under this bill, unauthorized access which caused injury would be punishable as a felony or misdemeanor. Because injury is so broadly defined, all first time hackers could be found guilty of a felony.

8. Injury broadly defined

Injury is defined to include not only damage or destruction to the computer and its data but also "any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system...or data was or was not altered, deleted, damaged or destroyed by the access." Thus, the fact that a computer owner incurs some costs to insure that a computer was not altered would trigger a state prison felony penalty even if the offense involved was first time access by a

(More)

hacker. Arguably such verification would be necessary whenever unauthorized access occurs, thus every first offense without damage could be a felony.

9. Employee misuse

Under this bill, an employee who used a computer more than once for such personal projects as preparing a personal letter, maintaining a mailing list or recipe list, accessing computer data to use in a term paper, or sending computer messages to other employees, could be guilty of a felony, even if the use occurred after work and caused no injury. On the other hand, an employee who uses the employer's computer system or data within the scope of employment would not be violating the statute.

10. Confiscation of property

This bill would authorize law enforcement officers to seize, under warrant or without warrant incident to a lawful arrest, any computer, computer system, computer program, instrument, apparatus, device, plans, instruction, or written publication used in the commission of any crime established under this Act. After conviction and a hearing to determine property rights, the seized computer equipment, if owned or controlled by the person so convicted, or owned or controlled by a person or entity that knowingly allowed the use of the seized item in the commission of any computer crime prohibited by this bill, could be destroyed as contraband by the sheriff of the county in which the person was

(More)

convicted, or given to the county for its use or for donation to any other public entity or nonprofit corporation.

This provision of the bill would allow confiscation and destruction of a costly computer system owned by another as a penalty for a first time access which caused no injury and which may be disposed of as an infraction or misdemeanor.

It could be argued that the seizure of computers used for these offenses might unjustly affect other innocent persons who have a property interest in these computers.

****

Revised: 12-24-85

COMPUTER CRIME TASK FORCE

CHAIRMAN

Carl A. Pabst, Partner
Touche Ross & Co.
3700 Wilshire Blvd., Suite 600
Los Angeles, CA 90010

Telephone: 739-6201

MEMBERS

Sgt. Robert Brown
L.A. Co. Sheriff's Dept.
Forgery-Fraud Detail
11515 So. Colima Road
Los Angeles, CA 90012

Telephone: 946-7212

William F. Fahey
Asst. U.S. Attorney
Office of the U.S. Attorney
1200 U.S. Courthouse
312 North Spring Street
Los Angeles, CA 90012

Telephone: 894-2391

Steve Plafker
Electronic Crime Unit
District Attorney's Office
320 West Temple St., Room 780
Los Angeles, CA 90012

Telephone: 974-3949

Alice Hand
Los Angeles City Attorney
Room 219
429 Bauchet Street
Los Angeles, CA 90012

Telephone: 485-6681

Edgar Hayes, Director
L.A. County Data Processing Department
9150 East Imperial Highway
Downey, CA 90242

Telephone: 940-2901

Sandra Mann Lambert
Vice President, ADP Security
Security Pacific National Bank
611 North Brand Blvd., Mail Code 2-155
Glendale, CA 91203

Telephone: (818) 507-3071

Chief Roger Moulton
Redondo Beach Police Department
401 Diamond Street
Redondo Beach, CA 90277

Telephone: 379-2477

Roy Nakawatase
Los Angeles City Unified School
District
450 North Grand Avenue
Los Angeles, CA 90012

Telephone 625-5228

John A. Nickols
(Representing L.A. Area
Chamber of Commerce)
Director of Security, Times Mirror
Times Mirror Square
Los Angeles, CA 90053

Telephone: 972-5701

Captain William Poggione
Commander, Commercial
Crimes Bureau
L.A. County Sheriff's Dept.
211 W. Temple St., Rm. 710
Los Angeles, CA 90012

Telephone: 974-4350

John Pricz
Carter, Hawley, Hale Stores
Information Services
1600 N. Kraemer Blvd.
Anaheim, CA 92806

Telephone: (714) 520-1816

Carl Reynolds, Vice President
Communications and Data Processing
Hughes Aircraft Company
Post Office Box 9399
Building C05, M/S 2001
Long Beach, CA 90810

Telephone: 513-5620

Dr. Richard Savich
Associate Professor, School of Accounting
University of Southern California
Los Angeles, CA 90089-1421

Telephone: 743-6184

Larry R. White
Hughes Aircraft Company
P.O. Box 9399, Bldg. C-7
Mail Station 2062
Long Beach, CA 90810-0465

Telephone: 513-3317

Ed Zeitler
Vice President, ADP Security
Security Pacific National Bank
611 North Brand Blvd., Mail Code 2-155
Glendale, CA 91203

Telephone: (818) 507-3026

STAFF

[redacted]
DEBRA PARKER

CCJCC
783 Hall of Administration
500 West Temple Street
Los Angeles, CA 90012

Telephone: 974-8398

CCJCC2
CTLIST1-4
12-24-85

Rec'd 3-16-87

JOHN K. VAN DE KAMP
Attorney General

State of California
DEPARTMENT OF JUSTICE

1515 K STREET, SUITE 511
P.O. BOX 944255
SACRAMENTO 94244-2550
(916) 445-9555

March 13, 1987

Honorable Ed Davis
Senator, 19th District
State Capitol, Room 2048
Sacramento, CA 95814

Dear Senator Davis:

Re: SB 255 - Computer Crime

The Attorney General's office supports SB 255.

This bill would repeal and reenact Penal Code section 502 relating to computer crimes. In so doing, it will make significant changes in the following areas:

1. Definitions. The definitions in SB 255 are broader than current law and directed more toward computer users than lawyers. Newly defined terms include "supporting documentation" and "injury."

The bill sets out seven species of crimes and reaches conduct that is not covered under existing 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, replicating current law.

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.

2. Punishment. Punishments generally remain the same as under current law: alternative felony/misdemeanor "wobbler" sentences are provided for most violations, the maximum felony punishments being 16 months, two or three years, and the maximum fine being $10,000. A first violation of subdivision (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 services, are punishable as felonies.

3. Collateral remedies. The collateral remedy provisions in 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 non-profit corporation as deemed appropriate by the court.

This is an excellent, comprehensive bill which clarifies and broadens existing law. If we can be of further assistance in supporting the bill, please let me know.

Very truly yours,

JOHN K. VAN DE KAMP
Attorney General

Michael L. Pinkerton
Deputy Attorney General

MLP:cj

SB 255

Date of Hearing: June 1, 1987
Counsel: DeeDee D'Adamo

ASSEMBLY COMMITTEE ON PUBLIC SAFETY
Larry Stirling, Chair

SB 255 (Davis) - As Amended: May 21, 1987

PRIOR ACTION: Senate Judiciary: 7 ayes; 0 noes
Senate Floor: 31 ayes; 0 noes

ISSUE:

I. SHOULD PROVISIONS OF LAW REGARDING COMPUTER CRIMES BE REPEALED AND REDEFINED?

II. SHOULD THE PENALTIES BE INCREASED FOR ONE WHO KNOWINGLY AND WITHOUT PERMISSION ACCESSES A COMPUTER WHEN AN INJURY RESULTS?

III. SHOULD FORFEITURE OF COMPUTER EQUIPMENT WHICH WAS USED TO COMMIT A COMPUTER CRIME BE AUTHORIZED?

DIGEST

Current law

1) Makes it an alternate felony/misdemeanor for one to intentionally access a computer for the purpose of defrauding.

2) Makes it an alternate felony/misdemeanor for one to maliciously access, alter, damage, or disrupt the operation of a computer system.

3) Makes it an infraction for one to intentionally and without authorization access a computer system. An act which results in injury and second offenses are punishable as an alternate felony/misdemeanor.

4) Defines computer terms, such as "computer program", "access", and "data".

5) Provides that the owner or lessee of a computer may bring a civil action for damages against one convicted of using his or her computer to commit a computer crime, and that such damages include expenditures incurred to verify that a computer was or was not altered, damaged, or deleted by the access.

6) Authorizes the court to award attorney's fees to a prevailing plaintiff in such civil actions.

This bill would:

1) Recast and redefine provisions of law relating to computer crimes.

2) Contain statements of legislative intent regarding the need to expand the provisions of law relating to computer crime.

3) Expand the definition of computer terms, and define additional computer terms, such as "supporting documentation" and "victim expenditure".

4) Provide that one who knowingly and without permission uses a computer is guilty of a misdemeanor for a first offense which does not result in injury and in which the value of the computer services does not exceed $400. Second offenses and first offenses which result in injury or in which the value of computer services is over $400 are punishable as an alternate felony/misdemeanor.

5) Increase the penalties for the unauthorized access of a computer.

6) Authorize the forfeiture, as specified, of a computer used to commit a computer crime.

7) Specify that for purposes of bringing a criminal action, a person who accesses a computer in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer in each jurisdiction.

COMMENTS

1) Purpose. According to the American Bar Association, as of June, 1984, 25% of America's largest companies suffer annual losses attributable to computer crime of between $145 and $730 million. This bill was developed by Los Angeles County's Computer Crime Task Force in order to provide for increased penalties for computer "hackers" and to provide standardized definitions of terms.

2) Penalties.

   a) Bill Increases Penalties for "Hackers." Under current law, one who accesses a computer is guilty of an infraction. Acts which result in injury and second offenses are punishable as misdemeanors. This bill would make acts which result in a victim expenditure (see comment 4j) of greater than $5,000 would be punishable as a misdemeanor or a felony.

   With respect to victim expenditures, the misdemeanor and felony penalty sections of this bill are both limited to injuries of greater than $5,000. Since there is no difference between these two sections, the bill should be amended to incorporate these provisions in the same section as alternative penalties, or to limit the misdemeanor provision to cases where the victim expenditure was under $5,000.

b) Penalties for Unauthorized Use. This bill would make it a crime to knowingly and without permission use a computer including, for example, an employee who uses his or her computer or a colleague's computer to write a term paper. Such acts are punishable as a misdemeanor where no injury results and where the value of the computer services does not exceed $400. Second offenses, or first offenses where the value of the computer services exceeds $400 or where injury results are punishable as an alternate felony/misdemeanor.

c) Other Computer Crimes. All other computer crimes (see Digest #1 and #2) are punishable as an alternate felony/misdemeanor. These penalties are the same as under current law.

3) Fines. Generally, up to a $1,000 fine can be imposed for one convicted of a misdemeanor. This bill provides that persons convicted of a misdemeanor computer crime offense can be fined up to $5,000. A fine up to $10,000 can be imposed for persons convicted of a felony.

4) Definitions of Terms.

a) Access is defined as gaining entry, instructing, or communicating with a computer.

b) Computer Network is defined as two or more computer systems connected by telecommunication facilities.

c) Computer Program or Software is defined as a set of instructions or statements which cause a computer to perform specified functions.

d) Computer services is defined as computer time, data processing, storage functions or other uses of a computer.

e) Computer system is defined as a device which contains computer programs, electronic instructions, input data, and output data, that performs such functions as logic, arithmetic, data storage and communication.

f) Data is defined as a representation of information, knowledge, facts, concepts, computer software, computer programs or instructions.

g) Supporting Documentation is defined as all information pertaining to the design, construction, classification, implementation, use of a computer which is not generally available to the public and is necessary for the operation of a computer.

h) Injury is defined as any alteration, deletion, damage, or destruction of a computer caused by the access.

i) Victim expenditure is defined as any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system was or was not altered or damaged by the access.

5) Employee Misuse. This bill exempts employees who were acting within the "scope of employment" from criminal liability. This provision would have the effect of authorizing an employee acting under the directive of his or her employer to access a computer in order to commit a fraud.

6) Seizure and Forfeiture of Computers. This bill would authorize law enforcement officers to seize computer equipment or plans or instructions used to commit a computer crime. This bill would authorize, upon conviction, the destruction of such items as contraband, or would authorize the sheriff of the county in which the person was convicted to use such items.

a) Opposition. The American Civil Liberties Union believes that it is sufficient for a person to be convicted, fined and incarcerated, and that the provision which allows the computer to be acquired by the county is tantamount to a bounty.

b) Seizure Provisions Only Apply to Owners of Computer Equipment. The seizure and forfeiture provisions of this bill only apply to owners of computer equipment who were either convicted of a computer crime or who allowed their equipment to be used in the commission of a computer crime.

In order to clarify that a conviction is required, this bill should be amended to specify that the person who used the owner's equipment must be convicted before the forfeiture is authorized.

c) Hearing Required. This bill would require a hearing to determine property rights before the seized computer equipment can be subject to forfeiture.

SOURCE: Los Angeles County Board of Supervisors

SUPPORT: None on file

OPPOSITION: American Civil Liberties Union