
Katja C. DeGroot

Follow this and additional works at: http://digitalcommons.law.scu.edu/chtlj

Part of the Law Commons

Recommended Citation
Available at: http://digitalcommons.law.scu.edu/chtlj/vol6/iss2/1

This Other is brought to you for free and open access by the Journals at Santa Clara Law Digital Commons. It has been accepted for inclusion in Santa Clara High Technology Law Journal by an authorized administrator of Santa Clara Law Digital Commons. For more information, please contact sculawlibrarian@gmail.com.
AN OVERVIEW OF RECENT CHANGES IN CALIFORNIA COMPUTER CRIME LAWS:


I. INTRODUCTION

In response to the growing proliferation of destructive “computer viruses,” the California Legislature recently enacted a stringent law designed to criminalize the introduction of these and other forms of electronic contaminants. Clarifying previous ambiguity in California laws dealing with computer crime, the Legislature amended Section 502(c) of the California Penal Code to make it a public offense to intentionally introduce a computer contaminant. In addition, the Legislature enacted companion legislation in the form of innovative deterrence measures designed to discourage computer “hackers” from creating and introducing high-tech electronic contaminants and from otherwise accessing computers to commit criminal acts. California Penal Code Section 502(g) adds a forfeiture provision mandating dispossessing of a defendant’s property interest in computers used during the commission of a computer crime, or used as a repository for the storage of illegally obtained software or data. Similarly, Section 1203.047 is added to the Penal Code to allow granting of probation for convicted computer criminals. During the probation period, the defendant is restricted from accepting employment where he or she would use a

---

3. See discussion infra p. 137.
5. Id. § 502(g); Id. § 502.01.
6. Id. § 1203.047.
computer connected by any means to any other computer.\textsuperscript{7}

The following summary highlights significant changes in and additions to current California laws dealing with computer crime. It provides a brief overview of Penal Code Section 502(c)(8), one of the nation’s toughest laws\textsuperscript{4} designed to deter the unleashing of electronic viruses. In addition to discussing the extent of the newly enacted antiviral legislation, it will examine the new penalty provisions under Penal Code Sections 502(g) and 1203.047 for convicted computer criminals.

II. THE CRIMINALIZATION OF COMPUTER VIRUS CONTAMINATION\textsuperscript{9}

A. Legislative Purpose

In both the original and amended versions of Penal Code Section 502, the California Legislature states its purpose as follows:

It is the intent of the Legislature in enacting this section to expand the degree of protection afforded to individuals, businesses and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems.\textsuperscript{10}

The Legislature found that a significant increase in computer crime accompanied the rapid growth of computer technology.\textsuperscript{11} It further found that protecting the integrity of all types of computer systems and computer data is vital in securing the economic and privacy interests of those persons and entities who lawfully use computers.\textsuperscript{12}

In amending Section 502 to specifically criminalize the introduction of computer contaminants, the California Legislature recognized that computers are an integral part of society and that the

\textsuperscript{7} Id.
\textsuperscript{8} For a comparison of computer crime laws, see ILL. REV. STAT. ch. 38, ¶ 16D-1 (Smith-Hurd 1989); CONN. GEN. STAT. ANN. § 53a-251b (West 1987); TEXAS PENAL CODE ANN. § 33.03 (Vernon Supp. 1989).
\textsuperscript{9} There exists some criticism about the use of criminal sanctions to deal with computer contamination. The contention is that the more stringent the laws are, the more likely computer criminals will try to challenge and evade them. Such critics argue that a more effective means for combatting the influx of viruses is through educational and technological alternatives. Such alternatives include providing mandatory “responsible computing” classes for students and professionals, promoting safe computing practices in the computing community, and utilizing antiviral “vaccines,” virus protection programs and screening procedures. The Scoop on Macintosh Viruses: Their History, Identification, and Edification, MacWorld, November, 1988 at 99.
\textsuperscript{10} CAL. PENAL CODE § 502(a) (West 1988).
\textsuperscript{11} Id.
\textsuperscript{12} Id.
phenomenon of computer virus contamination significantly threatens the reliability of those systems and data.

B. Perceived Inadequacy of Prior Computer Crime Law

Section 502(c)(4) makes it a crime to intentionally access and without permission add, alter, damage, delete, or destroy any data, computer, computer system, or computer network. Section 502(c)(5) makes it a crime knowingly and without permission to disrupt or cause the disruption of computer services. Although these laws aim to prevent unauthorized access to and interference with computer systems, the pre-amendment version of Section 502(c) had not made planting a destructive virus expressly illegal. Furthermore, it failed to explicitly define what constitutes a "computer contaminant." Thus, it was not clear whether a person who maliciously introduced a computer virus into a system could be prosecuted under the prior law. These shortcomings worried prosecutors and industry leaders who were intent on protecting the integrity of computer systems and electronic data. The ambiguity in the section motivated them to lobby for a law expressly criminalizing computer virus contamination.

C. Express Provision Covering Computer Contaminants

The addition of Penal Code Section 502(c)(8) clarifies that it is illegal for any person to "knowingly [introduce] any computer contaminant into any computer, computer system, or computer network."  

---

13. Id. § 502(c)(4).
14. Id. § 502(c)(5).
15. There have been no successful prosecutions under the prior section. However, not all prosecutors felt the old law was insufficient. Kenneth Rosenblatt of the Santa Clara County District Attorney's Office assisted in writing the new legislation. He believes that prosecution of virus contamination was possible under the pre-amendment Section 502(c), but recognized the need for an express provision. Telephone interview with Kenneth Rosenblatt, Santa Clara County District Attorney's Office, San Jose, California (Dec. 14, 1989).
16. For example, the Software Development Council, a Bay Area software developer/legal task force, has lobbied extensively for antiviral legislation. San Jose Mercury News, October 2, 1988, at 1F.
17. Networks are particularly vulnerable to attack. Local Area Networks (LAN's) and Wide Area Networks (WAN's), which link computer systems together to facilitate communication, serve as efficient conduits for contaminants. P. FITES, P. JOHNSTON & M. KRATZ, THE COMPUTER VIRUS CRISIS 11 (1989).
1. Definition of "Computer Contaminant"

Amended Penal Code Section 502(b)(10) defines a "computer contaminant" as:

any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms,\(^1\) which are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network.\(^2\)

The definition thus clarifies prior ambiguity in the law concerning the illegality of computer contamination.

2. Penalties

For a first violation which does not result in injury,\(^2\) a person found guilty of intentionally introducing a computer virus is subject to an infraction punishable by a fine not exceeding two hundred and fifty dollars.\(^2\) For a second violation or a violation which results in victim expenditure in an amount less than five thousand dollars, the defendant can be fined up to five thousand dollars and/or be sentenced to county jail for up to one year.\(^2\) Finally, for any violation which results in victim expenditure greater than five thousand dollars, a defendant may be fined up to ten thousand dollars, and/or be sentenced to state prison for up to three years.\(^2\)

Section 502(c)(8) does not apply to any person who accesses his or her employer's computers when acting within the scope of his or her employment.\(^2\)

---

1. Computer "worms" are malicious programs designed to move or "worm" their way through a computer program to alter or destroy data. P. FITES, P. JOHNSTON & M. KRATZ, THE COMPUTER VIRUS CRISIS 155 (1989).


21. An "injury" constitutes any alteration, deletion, damage, or destruction of a computer system, computer network, computer program, or data caused by the access. \(\text{id.} \) § 502(b)(8).

22. \(\text{id.} \) § 502(d)(3)(A).

23. \(\text{id.} \) § 502(d)(3)(B).

24. \(\text{id.} \) § 502(d)(3)(C). The section provides for an alternate sentence of up to one year in county jail and/or a fine not exceeding five thousand dollars. \(\text{id.} \)

25. \(\text{id.} \) § 502(b)(1). In fact, Subdivision (c) of Penal Code Section 502 does not apply to
III. INNOVATIVE PENALTIES "WITH A BYTE"

The recently enacted legislation is significant because it focuses on deterring computer crime in general. More than contributing the antiviral law, it expands and strengthens punishment for computer crimes through powerful and innovative criminal penalty provisions. The vast majority of computer criminals use computers to defraud or otherwise wrongfully obtain money, property or data, rather than to vandalize computer systems and data for its own sake. By developing stringent penalties, the Legislature responds to the growing problem of computer crime by focusing on deterring criminals from using computers to commit public offenses, as defined by Penal Code Section 502(c).

In determining an appropriate penalty for a person convicted of a violation of Section 502(c), a court is directed to consider prohibitions on access to and use of computers. Section 502(k) grants the court the flexibility to evaluate the defendant's remorse.

any employee who accesses his or her computer system when acting within the scope of his or her lawful employment. Id. See infra n.27.


27. CAL. PENAL CODE § 502(c) (West 1988 & Supp. 1990) defines the following as punishable public offenses:

(1) 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, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

(2) 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.

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

(4) 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.

(5) 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.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

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

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

and his or her recognition of wrongdoing. Furthermore, the court may consider alternatives to sentencing, such as community service.

A. Forfeiture Provisions

In addition to providing for fines and imprisonment, establishing civil remedies, authorizing an award of attorney fees, and providing for student disciplinary actions, the new legislation authorizes the forfeiture of a computer criminal's property interest in computers and computer software. Penal Code Section 502(g) provides that:

any computer, computer system, computer network, or any software or data, owned by the defendant, which is used during the commission of any public offense described in subdivision (c) of Section 502 or any computer, owned by the defendant, which is used as a repository for the storage of software or data illegally obtained in violation of subdivision (c) shall be subject to forfeiture.

Further, the law specifies that if the defendant is a minor, the items subject to forfeiture include property of the parent or guardian. As do traditional forfeiture provisions, this law threatens to take away the "tools of the trade."

As a protective measure, Section 502.01 provides for a hearing to identify those persons, other than the defendant, who have a

---

29. Id. § 502(k)(2).
30. Id.
31. Id. § 502(d).
32. Id.
33. "In addition to any other civil remedy available, the owner or lessee of the computer ... may bring a civil action against any person convicted [under Section 502(o)] for compensatory damages, including any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer ... was not altered, damaged, or deleted by the access." Id. § 502(e)(1).
34. Id. § 502(e)(2).
35. CAL. PENAL CODE § 502(e)(3) (West Supp. 1990) requires community colleges, state universities and state-accredited academic institutions to include computer-related crimes as a specific violation of student policies which may subject the student to disciplinary action. The subsection applies to the University of California upon resolution by the Board of Regents. Id. § 502(e)(3).
36. Id. § 502(g). CAL. PENAL CODE § 502.01 defines the property used by the defendant in committing a criminal offense in violation of Section 502 that is subject to forfeiture. Id. § 502.01.
37. Id. § 502.01(e). The computer and related software will not be subject to forfeiture if the parent swears that the minor child shall not have access to any computer owned by the parent for two years after the sentencing date. Id.
valid interest in the property subject to forfeiture. If, after filing a motion for redemption of interest, a party is identified as holding an interest in the computer or software, he or she may be entitled to the property. If the defendant is found to have the only valid interest in the property, the property shall be distributed first to the victim, if the victim elects to accept it as restitution for the injury, and residually, to the agency responsible for investigating or prosecuting the offense.

B. Prohibiting Access to Computers

Penal Code Section 1203.047 contains the new legislation's most promising and interesting deterrent measure. The section allows a judge to grant probation for not less than three years. Most significantly, for the duration of the probation period, the convicted computer criminal "shall not accept employment where that person would use a computer connected by any means to any other computer." A court may make an exception and authorize employment using computers if it finds that the proposed employment would not pose a threat to the public. In determining whether employment of the defendant would pose a risk, the court must provide notice to, and an opportunity to be heard by, interested parties. Thus, a current or potential employer will always know that the defendant was convicted of a computer-related crime. In effect, the restrictions on employment during the probationary period remove the defendant from his vocation and livelihood. Because the

38. Id. § 502.01(c).
39. Id. § 502.01(d)(3). The court determines the value of the property and the value of each valid interest in the property. If the value of the property is greater than the value of the interest, the holder of the interest is entitled to the property upon paying the court the difference between the value of the property and the value of the interest. If the value of the interest is greater than the value of the property, the property will be sold and the owner of the interest will receive the proceeds. Id. § 502.01(d)(4).
40. Id. § 502.01(f)(1).
41. Id. § 502.01(f)(2).
42. The new legislation also added Section 1203.048 to the Penal Code. It provides that, except in unusual cases, a judge must not grant probation to any person convicted of violating Section 502 if the crime involved the taking of or damage to property valued in excess of one hundred thousand dollars. Id. § 1203.048.
43. Id. § 1203.047. The section allows for a shorter probation period "where the ends of justice would be better served." Id.
44. Id. § 1203.047. By its language, the scope of the prohibition is very broad. A defendant would be prohibited from securing employment in any business or profession, whether or not it is related to a high technology industry.
45. Id.
46. Id.
penalty is so narrowly tailored to the computer criminal, it promises
to be a very effective measure to deter computer crime.

IV. Conclusion

The California Legislature added Section 502(c)(8) to the Cali-
ifornia Penal Code to clarify that it is illegal knowingly to introduce
a computer contaminant into a computer system. More signifi-
cantly, it added Section 502(g) which mandates forfeiture of a con-
victed defendant's property interest in computers and Section
1203.047 which places limitations on employment while a convicted
computer criminal is on probation.

The amended Section 502(c) and the new penalty provisions
are expected to deter computer virus contamination and computer
crime dramatically. By clarifying the computer crime laws, and by
tailoring the penalties to computer criminals, the California Legisla-
ture has demonstrated its commitment to protecting the public's in-
terest in preserving the integrity of computers, computer systems,
and computer data.

Katja C. DeGroot