

**People v. Lawton (1996) 48 Cal.App.4th Supp. 11 , 56
Cal.Rptr.2d 521**

[No. 94C006560. Appellate Department, Superior Court, Ventura Jul 16, 1996.]

THE PEOPLE, Plaintiff and Respondent, v. JEFFREY LAWTON, Defendant and Appellant.

(Municipal Court of Ventura County, No. 94C006560, John R. Smiley, Judge.)

(Opinion by O'Neill, J., with Storch, P. J., and Peck, J., concurring.)

COUNSEL

Jill C. Hatfield for Defendant and Appellant.

Michael D. Bradbury, District Attorney, and Miles Weiss, Deputy District Attorney, for Plaintiff and Respondent.

OPINION

O'NEILL, J.

We affirm a conviction for unauthorized access to a computer system, and hold that such an offense can be committed by use of a public access terminal to bypass security and penetrate levels of software not open to the public.

The Case

Jeffrey Lawton (Appellant) was charged with three computer-related crimes, as defined in Penal Code section 502. The jury hung on charges of altering or damaging data (Pen. Code, § 502, subd. (c)(4)) and disrupting computer services (Pen. Code, § 502, subd. (c)(5)). Appellant was convicted of violating Penal Code section 502, subdivision (c)(7), which forbids unauthorized access to "any computer, computer system, or computer network." Probation was granted, and this appeal followed.

The Facts

The Ventura County Library Services Agency utilizes a mainframe computer with over 200 terminals, a number of which are located in the Camarillo Public Library. Terminals are available for use by library patrons for the sole purpose of accessing the computerized catalog of books. Other portions of the software, containing such information as patrons' names, [48 Cal.App.4th Supp. 13] addresses, phone numbers and driver's license numbers, are closed to the public by a security system that includes employee passwords.

At three different times on May 11, 1994, Appellant was seen by a Camarillo library employee, Ms. Delgado, at or near three different public computer terminals. During the first encounter, Ms. Delgado noticed that terminal No. 1 was "off-line," displaying scrambled letters and numbers not part of the software accessible to the public. Fifteen minutes later she noticed Appellant at terminal No. 1. When she asked Appellant to move aside he entered a series of key strokes including the word "abort." The display then came back "on-line" in the public data area.

After this incident Appellant moved toward the magazine room, where terminal No. 2 is located. Ms. Delgado did not see Appellant enter, but she did see him in the magazine room five minutes later. Her supervisor, Ms. Bell, saw Appellant at terminal No. 2. Thirty minutes after the problem with terminal No. 1, Mrs. Delgado noted that terminal No. 2 was running a "prime number" check, displaying a scrolling column of six-to seven-digit numbers. Ms. Delgado and Ms. Bell were unable to bring terminal No. 2 back on-line, and the problem was referred to the automation department.

Later the same day Ms. Delgado saw Appellant sit down at terminal No. 3 in the same library. She approached and watched as Appellant "knocked" the terminal off-line from the public access software level. She told Appellant what he was doing was illegal. He apologized and brought the terminal back on-line by a series of key strokes.

The computer system's self-monitoring program recorded numerous unusual commands from at least three Camarillo library terminals on the date in question. They reveal that someone accessed both the operating system (UNIX) and the "Universe," or database, level. A number of specific commands were entered, such as the prime number check, a command designed to slow down the computer by tying up processing power, and "DUA," which results in a display of user passwords entered by others trying to log on to the system. Ms. Everson, the Ventura County information systems support analyst assigned to the library system, analyzed the record of unusual commands. She concluded that someone on that date was seeking passwords and other information in an attempt to gain more access to the system. She also noted that two different commands were entered with potential to purge data from the system. The weekly system check immediately after the date in question revealed some missing temporary data files, an event unique in her six years of managing the system. She attributed the **[48 Cal.App.4th Supp. 14]** deletions to the unusual commands entered at the Camarillo library on May 11, 1994. Specifically, the commands which could have purged data were "RM" (standing for "Remove") and "Clean.Account." She believes the latter command caused the deletions.

Experts called by each side debated the merits of the library computer system's security and the significance of the various unusual commands recorded by the self-monitoring program. The defense expert concluded that someone with surface knowledge of the UNIX system could have accidentally penetrated to the lower levels of the software due to a bug in the library's software. He conceded that temporary data may have been deleted as a result of the "Clean.Account" command, and that, unless that command was selected from a menu, it would not have been entered as the result of random keystrokes.

The prosecution expert found the security "perfectly adequate" for a library system. The "Remove" command is a powerful one, capable of erasing almost anything. It was entered but probably not executed, since "nothing important" had been deleted. The temporary files that were deleted covered the time period March 30 to May 11. This erasure was consistent with execution of the "Clean.Account" command by someone trying to "cover their tracks."

Appellant, an unemployed aerospace software engineer, told the sheriff's deputy who investigated that he did go "way beyond the application" by utilizing an invalid code and a "little trap door." He stated that his motivation was "partly out of curiosity" and also to learn about the UNIX system to "help my career."

The Appeal

The only issue pursued on appeal is the contention that the evidence at trial was insufficient as a matter of law, because one who uses a computer terminal with permission cannot as a matter of law violate Penal Code section 502, subdivision (c)(7). The People contend that permissible use of hardware to access impermissible levels of software is a violation of that section.

Discussion

Penal Code section 502 was amended in 1987 to expand the protection of "the integrity of all types and forms of lawfully created computers, computer [48 Cal.App.4th Supp. 15] systems, and computer data," which the Legislature found "vital... to the well-being of ... governmental agencies, and others within this state." (Pen. Code, § 502, subd. (a).) Subdivision (c) of the statute is a laundry list of illegal activity ranging from use of a computer to defraud or extort, to infecting a computer with a virus. As mentioned earlier, subdivision (c)(7) covers one who "knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network."

Subdivision (b) of Penal Code section 502 defines various terms used therein, not including the single word "computer." Subdivision (b)(5) defines "computer system" as "... a device or collection of devices, including support devices ..., 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." Subdivision (b)(2) defines "computer network" as "... any system which provides communications between one or more computer systems and input/output devices including, but not limited to, display terminals and printers connected by telecommunication facilities."

To paraphrase the statute, a "computer system" is a functioning combination of hardware and software. A "computer network" is the hardware and software which links one or more systems with each other and/or with terminals and printers.

In other words, we read both "computer system" and "computer network" as consisting of hardware and software.

Accordingly, we reject Appellant's contention that subdivision (c)(7) of Penal Code section 502 covers only unauthorized access of hardware. Such an interpretation would not only clash with the statutory language quoted above, but with the overall statutory intent to comprehensively protect the integrity of private, commercial, and governmental computer systems and data. (See Pen. Code, § 502, subd. (a).)

A review of the various provisions of Penal Code section 502, subdivision (c) reveals that adopting Appellant's argument would carve a giant loophole in the statute not intended by its drafters. Public access computer terminals are increasingly common in the offices of many governmental bodies and agencies, from courthouses to tax assessors. We believe subdivision (c)(7) was designed to criminalize unauthorized access to the software and data in such systems, even where none of the other illegal activities listed in subdivision (c) have occurred. **[48 Cal.App.4th Supp. 16]**

To the extent that "mere browsing" in this fashion may cause little or no harm, the statute appropriately sets modest penalties for unaggravated behavior which violates Penal Code section 502, subdivision (c)(7). (See Pen. Code, § 502, subd. (d)(3).)

We affirm the conviction and order granting probation.

Storch, P. J., and Peck, J., concurred.

[End of volume 48 Cal.App.4th]