Filed 7/15/24

**CERTIFIED FOR PUBLICATION**

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA

FIRST APPELLATE DISTRICT

DIVISION THREE

| | |
|---|---|
| In re JOSE OLIVERAS on Habeas Corpus | A168677<br><br>(Del Norte County Super. Ct. No. HCPB235049) |

Petitioner Jose Oliveras challenged a disciplinary sanction revoking his computer access and rendering him ineligible for computer-access-required work assignments or programming because of being found with contraband pornographic images on a tablet device.

We issued an order to show cause to the Secretary of the Department of Corrections and Rehabilitation (Secretary), requesting in part they address whether Oliveras's conduct violated Penal Code section 502.[1] In response, the Secretary asserts the petition is moot because Oliveras's computer clearance was reauthorized. We disagree and order the Secretary to vacate any reference to a section 502 and/or "computer fraud and abuse" violation from Oliveras's record.

## BACKGROUND

Oliveras is currently serving a life sentence without the possibility of parole following his 2012 conviction for kidnapping, first degree murder,

[1] All undesignated statutory references are to the Penal Code.

kidnapping for ransom, conspiracy to commit a crime, and various gang and weapons enhancements.

Certain prisoners, including Oliveras, are provided with electronic tablets to allow them to access certain services and communicate with family. During an inspection of a tablet assigned to Oliveras for his use, an investigative services unit officer discovered over 600 pornographic images. The images were stored on a removable SIM (Subscriber Identity Module) card.[2] In response, Oliveras was charged with a violation of California Code of Regulations (CCR), title 15, section 3006(c) for "possession of contraband," i.e., obscene material. That section provides, "Except as authorized by the institution head, inmates shall not possess or have under their control any matter which contains or concerns any of the following . . . Obscene material . . . ." (Cal. Code Regs., tit. 15, § 3006, subd. (c) (CCR section 3006(c)).) The tablet was forwarded to the Correctional Intelligence Task Force for an additional investigation into possible illicit activity, but no additional violations were noted or charged.

Oliveras pled guilty to the administrative violation charge and received counseling for misconduct "without reprimand." The hearing officer did not make any findings regarding whether Oliver was "a program failure" and did not issue a referral to a classification committee for program review.

Approximately eight months later, in October 2022 at Oliveras's annual classification review hearing, a Unit Classification Committee rescinded

---

[2] We refer to the device as a "SIM card" because that is the terminology used in the record. However, the description of the device—an external storage card that was inserted into the tablet—appears to describe a device more analogous to a SD (Secure Digital) card. The record is silent as to (1) how the images came to be stored on the SIM card, and (2) whether Oliveras used the tablet to access the images.

Oliveras's computer clearance "due to disciplinary [sic]." The only disciplinary behavior identified in the review was Oliveras's administrative violation for possession of contraband. In its discussion of computer clearance, the committee "noted" the circumstances of the violation and stated, "CCR, Title 15, Sections 3040(h) and 3041.3(j) state that inmates who have a history of computer fraud or abuse, including documented institutional disciplinary action involving computer fraud or abuse, shall not be placed in any work assignment that provides access to a computer, or rehabilitative program which provides access to the internet. Because an electronic tablet is essentially a hand-held computer and performs many of the same tasks as a desktop or laptop computer, [the committee] finds it appropriate to rescind [Oliveras's] computer clearance and remove him from any wait lists for programs or job assignments that would allow him computer access."

Oliveras subsequently filed a grievance with the Department of Corrections and Rehabilitation (CDCR). He asserted the tablet in his possession did not provide any meaningful laptop or desktop functions and his rule violation for possession of contraband did not constitute " 'computer fraud or abuse' " as defined in the Penal Code. He noted he had recently been accepted in the "the next cycle of the prestigious Last Mile computer coding program," in which he could now no longer participate. The CDCR denied both his grievance and his subsequent appeal.

Oliveras filed a petition challenging this reclassification with the superior court. The court noted the hearing officer's decision "will be upheld as long as there is 'some basis in fact' for the decision." The court then denied the petition, explaining "[t]he hearing officer's findings that denial of access to computers or work assignments is an appropriate sanction is supported by

'some evidence' in the record." The court did not identify what evidence it was referencing.

In September 2023, Oliveras filed the pending petition. In October 2023, while his petition was pending, prison officials conducted Oliveras's annual classification committee review hearing and reauthorized his computer clearance. In January 2024, this court issued an order to show cause, requesting in part the Secretary address (1) whether Oliveras introduced pornography onto his tablet "without permission" as defined under section 502, and (2) whether Oliveras's conduct violated section 502.

## DISCUSSION

### I. Mootness

The Attorney General argues the matter is moot because the classification committee has since reauthorized Oliveras for computer clearance.

"A case is moot when the reviewing court cannot provide the parties with practical, effectual relief." (*City of San Jose v. International Assn. of Firefighters, Local 230* (2009) 178 Cal.App.4th 408, 417.) Likewise, "[t]he voluntary cessation of allegedly wrongful conduct destroys the justiciability of a controversy and renders an action moot unless there is a reasonable expectation the allegedly wrongful conduct will be repeated." (*Ctr. for Loc. Gov't Accountability v. City of San Diego* (2016) 247 Cal.App.4th 1146, 1157.) The underlying policy behind the mootness doctrine is that courts decide justiciable controversies and do not normally render merely advisory opinions. (*Ebensteiner Co., Inc. v. Chadmar Group* (2006) 143 Cal.App.4th 1174, 1178–1179.)

However, mootness may be considered alongside the purposes of habeas corpus and the courts' concomitant "broad remedial powers" to afford relief.

(See *People v. Aragon* (1992) 11 Cal.App.4th 749, 760.) The court may dispose of a habeas corpus petition in the manner justice requires, with the flexibility to correct miscarriages of justice. (*In re Brindle* (1979) 91 Cal.App.3d 660, 669–670.) " ' "The very nature of the writ demands that it be administered with the initiative and flexibility essential to insure that miscarriages of justice within its reach are surfaced and corrected." [Citation.] Extraordinary relief by mandamus or habeas corpus has been utilized to correct prior conditions or to declare the rights of unnamed and future petitioners by decisions designed to affect the prospective administration of the criminal justice system. [Citations.] "Where questions of general public concern are involved, particularly in the area of the supervision of the administration of criminal justice (the court) may reject mootness as a bar to the decision on the merits." [Citation.] Although the petitioner may have received the relief prayed for, the court nevertheless may decide a question arising from a recurring problem important to insure the basic rights of prisoners. [Citation.] Habeas corpus is an appropriate procedure to be used by petitioners "to obtain a declaration of rights in the prevailing circumstances." ' " (*In re Carr* (1981) 116 Cal.App.3d 962, 964, fn. 1.)

Here, Oliveras pled guilty to a specific rule violation—possession of contraband. At a subsequent classification committee review hearing, the committee considered that violation as a violation of two different regulations: CCR, title 15, sections 3040, subdivision (h) (CCR section 3040(h)), and 3041.3, subdivision (j) (CCR section 3041.3(j)), and imposed additional punishment by way of rescinding Oliveras's computer clearance. Although his computer clearance was recently restored, the Secretary acknowledges inmates may be subject to computer restrictions "if the inmate

has a history of computer fraud or abuse, including a documented institutional disciplinary action involving computer fraud or abuse." Nothing in the record indicates the CDCR will not continue to consider his administrative violation of CCR section 3006(c) (possession of contraband) as a violation of CCR sections 3040(h) and 3041.3(j) (computer fraud and abuse).

*In re Marti* (2021) 69 Cal.App.5th 561 is instructive. In that matter, an inmate challenged a decision finding him guilty of a prison disciplinary violation for possession of excess property. (*Id.* at p. 563.) While the CDCR asserted the issue was moot because the inmate had already "suffered the punitive consequences of the decision" and any future harm was speculative, the court disagreed as "the adjudication remains in [the inmate's] file and may be considered in the future, for example for purposes of classifying another violation as serious or administrative." (*Id.* at pp. 563, 567.) "Whatever the full scope of prison decisions that may be affected by adjudication of an administrative rules violation, it is clear this court can afford petitioner meaningful relief by vacating . . . [the] adjudication of the administrative rules violation." (*Id.* at p. 567.) As in *Marti*, the classification of Oliveras's administrative violation as "computer fraud or abuse" remains in his file and may be considered in future committee classification review hearings.

Accordingly, we will address the petition on the merits.[3]

---

[3] The Attorney General's return argued mootness but failed to address the merits of the petition. Generally, a return is supposed to frame the issues that are to be decided by the court. (*People v. Duvall* (1995) 9 Cal.4th 464, 476–477 ["The requirement that the return allege facts responsive to the petition is critical, for the factual allegations in the return are either admitted or disputed in the traverse and this interplay frames the factual issues that the court must decide."].) We need not address whether the Attorney General has forfeited its argument on the merits. It is undisputed that Oliveras pled guilty to the administrative charge of possessing

## II. Oliveras's Rule Violation

Although Oliveras was charged with, and pled guilty to, possession of contraband, the Classification Committee subsequently concluded Oliveras's violation constituted computer abuse and prohibited him from work assignments with computer or internet access.

### A. Standard of Review

Section 1094.5 of the Code of Civil Procedure governs judicial review by administrative mandate of any final decision or order rendered by an administrative agency. "Interpretation of a statute or regulation is a question of law subject to independent review." (*Christensen v. Lightbourne* (2017) 15 Cal.App.5th 1239, 1251 (*Christensen*); *United Artists Theatre Circuit, Inc. v Cal. Regional Water Quality Control Bd.* (2019) 42 Cal.App.5th 851, 865 (*United Artists*) [" 'where, as here, the determinative question is one of statutory or regulatory interpretation, an issue of law, we may exercise our independent judgment.' "].)

The principles of statutory interpretation are well-established. " 'Our fundamental task in interpretating a statute is to determine the Legislature's intent so as to effectuate the law's purpose. We first examine the statutory language, giving it a plain and commonsense meaning. We do not examine that language in isolation, but in the context of the statutory framework as a whole in order to determine its scope and purpose and to harmonize the various parts of the enactment. If the language is clear, courts must generally follow its plain meaning unless a literal interpretation would result in absurd consequences the Legislature did not intend. If the statutory

---

contraband, and we may decide, as a matter of statutory interpretation, whether the record supporting that charge establishes a violation of section 502. (See Part II, *post*.)

language permits more than one reasonable interpretation, courts may consider other aids, such as the statute's purpose, legislative history, and public policy.' [Citations.] ' "[T]he objective sought to be achieved by a statute as well as the evil to be prevented is of prime consideration in . . . interpretation, and where a word of common usage has more than one meaning, the one which will best attain the purposes of the statute should be adopted . . . ." ' " (*United Artists*, *supra*, 42 Cal.App.5th at p. 866.)

" '[W]here the meaning and legal effect of a statute is the issue, an agency's interpretation is one among several tools available to the court. Depending on the context, it may be helpful, enlightening, even convincing. It may sometimes be of little worth. [Citation.] Considered alone and apart from the context and circumstances that produce them, agency interpretation is not binding or necessarily even authoritative . . . . "The standard for judicial review of agency interpretation of law is the *independent judgment* of the court, giving *deference* to the determination of the agency *appropriate* to the circumstances of the agency action." ' [Citation.] 'Unlike quasi-legislative rules, an agency's interpretation does not implicate the exercise of a delegated lawmaking power; instead, it represents the agency's view of the statute's legal meaning and effect, questions lying within the constitutional domain of the courts. But because the agency will often be interpreting a statute within its administrative jurisdiction, it may possess special familiarity with satellite legal and regulatory issues. It is the "expertise," expressed as an interpretation . . . , that is the source of the presumptive value of the agency's views.' " (*Ibid.*)

**B. Analysis**

The California Code of Regulations provides "Inmates who have a history of computer fraud or abuse, including documented institutional

disciplinary action involving computer fraud or abuse, shall not be placed in any work assignment that provides access to a computer." (CCR § 3040(h); see also CCR § 3041.3(j) ["Inmates who have a record of computer fraud or abuse shall not be placed in any work assignment which provides access to a computer"].)

While neither CCR sections 3040 nor 3041.3 define "computer fraud or abuse," the Attorney General does not dispute it should be interpreted pursuant to section 502. The Attorney General contends CDCR Department Operations Manual section 49020.18.1 "provides guidance to employees to decide when an inmate commits computer abuse." That section states "[i]nmates who have a history of computer fraud or abuse, *as defined by Penal Code section 502*, shall not be placed in any assignment that provides access to a computer." (Italics added.) The agency's interpretation of the phrase "computer fraud or abuse" in CCR sections 3040 and 3041.3 pursuant to Operations Manual section 49020.18.1—i.e., as defined by Penal Code section 502—is not " 'clearly erroneous or unauthorized under the statute.' " (See *Christensen*, *supra*, 15 Cal.App.5th at p. 1252.) As such, we defer to the agency's interpretation and consider whether Oliveras's conduct and/or disciplinary action constituted "computer fraud or abuse" as defined by section 502.

In briefing before this court, the Attorney General asserts Oliveras's conduct constituted computer abuse under subdivisions (c)(1), (3)–(4), and (6)–(7) of section 502. These provisions provide as follows:

> "(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.
>
> . . .

> (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.
>
> . . .
>
> (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."

(§ 502, subds. (c)(1), (3)–(4), (6)–(7).)

As an initial matter, the plain language of subdivisions (c)(6) and (7) do not apply to Oliveras's conduct. Those provisions require Oliveras to have accessed a computer, computer system, or computer network "without permission." (§ 502, subds. (c)(6), (7).) The record reflects Oliveras was assigned the tablet at issue for his personal use, and he thus had permission to access the tablet and use the tablet functions contained thereon.

Likewise, the plain language of subdivision (c)(3) does not encompass Oliveras's conduct. That subdivision criminalizes use of "computer services"[4] without permission. (§ 502, subd. (c)(3).) Based on the record before this court, there is no evidence that Oliveras used any "computer services" on his tablet—such as internet access or email—to obtain the pornography or share the images with any third parties. Nor does the record indicate Oliveras transferred or stored any of the images directly onto his tablet from the SIM

---

[4] Section 502, subdivision (b)(4) defines " 'computer services' " as "includ[ing], but is not limited to, computer time, data processing, or storage functions, internet services, electronic mail services, electronic message services, or other uses of a computer, computer system, or computer network."

card. And though it may be that Oliveras could have used his tablet to view the images, nothing in the record actually indicates he did so. Under well-established appellate rules, we are "limited to consideration of the matters contained in the appellate record." (*People v. Neilson* (2007) 154 Cal.App.4th 1529, 1534.)

For similar reasons, subdivision (c)(1) also does not apply here. That provision requires Oliveras to have "knowingly and without permission" used data or computers for the purpose of either "devis[ing] or execut[ing] any scheme or artifice to defraud, deceive, or extort" or "wrongfully control[ling] or obtain[ing] money, property, or data." (§ 502, subd. (c)(1).) As noted in connection with subdivision (c)(3), the record is silent as to whether Oliveras used any function on his tablet to obtain the pornography or, once obtained, used the pornography for any purpose. More importantly, nothing in the record indicates the pornography discovered on Oliveras's tablet was used or connected to any illegitimate purpose, such as fraud or extortion.

Conceivably, Oliveras exerted "control"—a term not defined by section 502—over the pornography by mere possession. But non-injurious possession, without more, exceeds any reasonable interpretation of the statute.

At the time the Legislature enacted Senate Bill No. 255 (S.B. 255), which repealed and rewrote section 502, the Legislature was focused on increased harm to businesses caused by computer crimes. An Assembly analysis of S.B. 255 highlighted concerns regarding the significant financial losses suffered by America's companies "attributable to computer crime," and stated the bill "was developed by Los Angeles County's Computer Crime Task Force to provide for increased penalties for computer 'hackers' and to provide standardized definitions of terms." (Assem. Pub. Safety Com., 3d reading

analysis of Sen. Bill No. 225 (1987-1988 Reg. Sess.) as amended Sept. 8, 1987, p. 2.) The "legislative intent" behind the bill was "the need to expand the provisions of law relating to computer crime." (*Id.*, p. 1.) And specific discussions regarding subdivision (c)(1) indicate the Legislature's concern with "wrongful control" related to instances arising from "false pretenses." (Sen. Com. on Judiciary, Analysis of Sen. Bill No. 255 (1987-1988 Reg. Sess.) Feb. 27, 1987, p. 2; see also Assem. Pub. Safety Com. Republican Caucus, analysis of Sen. Bill No. 255 (1987-1988 Reg. Sess.) as amended Jun. 23, 1987 [summarizes subdivision (c)(1) as establishing criminal penalties for "using a computer to defraud or steal."].) Oliveras's conduct does not fall within the scope of conduct the Legislature sought to address.

*Van Buren v. United States* (2021) 593 U.S. 374 (*Van Buren*) provides an instructive analogy. In *Van Buren*, a police officer was authorized to access a license plate database for law enforcement purposes. However, the officer ran a license plate search in the database in exchange for money. The government subsequently charged the officer with violating the Computer Fraud and Abuse Act of 1986 (CFAA). The CFAA "subjects to criminal liability anyone who 'intentionally accesses a computer without authorization or exceeds authorized access,' and thereby obtains computer information." (*Van Buren*, at p. 379.) The parties disputed whether the phrase "exceeds authorized access" applied to improper use of authorized access or prohibited access. (*Id.* at pp. 382–383.) As relevant here, the Supreme Court noted the government's interpretation "would attach criminal penalties to a breathtaking amount of commonplace computer activity. . . . [¶] If the 'exceeds authorized access' clause criminalizes every violation of a computer-use policy, then millions of otherwise law-abiding citizens are criminals." (*Id.* at p. 393.) The court thus concluded "an individual 'exceeds authorized

access' when he accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or databases—that are off limits to him." (*Id.* at p. 396.) Because the officer was entitled to access the license plate database, the court held he "did not 'excee[d] authorized access' " under the CFAA, "even though he obtained information from the database for an improper purpose." (*Ibid.*)

We find a similar interpretation appropriate here. Oliveras, like the officer in *Van Buren*, was authorized to access his tablet for personal use and, presumably, maintain personal data on the device. Even if Oliveras utilized that authorized access for an improper purpose—i.e., placing a SIM card containing pornographic images into his tablet—he did not engage in the type of conduct section 502 was designed to criminalize.

Finally, subdivision (c)(4) criminalizes "add[ing], alter[ing], damag[ing], delet[ing], or destroy[ing] any data, computer software, or computer programs" without permission. (§ 502, subd. (c)(4).) Here, the question is whether placing a SIM card containing pornography into his tablet could qualify as "add[ing] . . . data" to his tablet "without permission."

Section 502 broadly defines "data" as "a representation of information, knowledge, facts, concepts, computer software, or computer programs or instructions." (§ 502, subd. (b)(8).) While pornography arguably falls within this definition, a SIM card—by itself—does not. A SIM card or memory card is external hardware, not "software." (Cf *In re Robinson* (2017) 19 Cal.App.5th 247, 254 [distinguishing between the external storage devices/memory cards and the software contained thereon].) Thus, the question is not whether Oliveras placed a SIM card into his tablet—which the record indicates he did—but whether he impermissibly added data from that SIM card onto his tablet.

The statute does not define the term "add" and, therefore, the phrase "add[ed] . . . data" is ambiguous. In the case before us, this ambiguity is of no import as we conclude the legislative history overwhelmingly indicates the Legislature did not intend to criminalize an individual for merely viewing images contained on a SIM card inserted into his own personal electronic device.

As discussed above, S.B. 255 was focused on addressing computer crime. In discussing the specific expansion of crimes encompassed by S.B. 255, the Legislature summarized subdivision (c)(4)—the provision at issue here—as creating criminal liability for "accessing, altering, damaging, etc. data, software, programs or supporting documentation, *in other words, vandalism*." (Sen. Com. on Judiciary, Analysis of Sen. Bill No. 255 (1987-1988 Reg. Sess.) Feb. 27, 1987, p. 2 (italics added); see also Assem. Pub. Safety Com. Republican Caucus, analysis of Sen. Bill No. 255 (1987-1988 Reg. Sess.) as amended Jun. 23, 1987 [summarizes subdivision (c)(4) as establishing criminal penalties for "vandalizing computer software and systems."].) The Legislature also expressly excluded from criminal liability an employee's use, knowingly and without permission, of an employer's computer outside an employee's scope of employment which does not result in an injury "to the employer or another." (§ 502, subds. (h)(2), (i).)

Given the above legislative history, we cannot reasonably conclude the Legislature intended an individual's use of a personal computer to view images saved on a memory card to qualify as impermissibly "adding data" under subdivision (c)(4). Rather, the record expressly indicates the legislative focus was vandalism, e.g., adding malware to a computer. Oliveras's conduct is more akin to an employee's improper but non-injurious use of an employer's computer, which the Legislature expressly excluded

from liability under section 502. (Accord *Van Buren*, *supra*, 593 U.S. at p. 396 [officer "did not 'excee[d] authorized access' " under the CFAA, "even though he obtained information from the database for an improper purpose."].)

In sum, considering the purpose of section 502 and its legislative history, we conclude the CDCR's finding that Oliveras's conduct constituted "computer fraud and abuse" is unpersuasive and we decline to adopt its interpretation. (See *United Artists*, *supra*, 42 Cal.App.5th at p. 866.) To the contrary, we conclude Oliveras's conduct did not constitute "computer fraud and abuse" under section 502, and improperly subjected him to discipline under CCR sections 3040 and 3041.3.

**DISPOSITION**

The October 2022 revocation of petitioner's computer clearance and removal from wait lists for programs or job assignments that would allow him computer access by the Unit Classification Committee is reversed and respondent is directed to remove any reference to this revocation from petitioner's file.

_____
Petrou, J.

WE CONCUR:

_____
Tucher, P.J.

_____
Fujisaki, J.

| | |
|---|---|
| Trial Court: | Del Norte County Superior Court |
| Trial Judge: | Hon. Robert Cochran |
| Counsel: | Rob Bonta, Attorney General, Sara J. Romano, Senior Assistant Attorney General, Amanda J. Murray, Supervising Deputy Attorney General, and John P. Walter, Deputy Attorney General, for Respondent.<br><br>First District Appellate Project, Donald H. Specter, for Petitioner. |