Filed 6/26/25

CERTIFIED FOR PUBLICATION

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA
SECOND APPELLATE DISTRICT
DIVISION FIVE

DIANA MARIA TERAN, Petitioner, v. THE SUPERIOR COURT OF LOS ANGELES COUNTY, Respondent; THE PEOPLE, Real Party in Interest.	B341644 (Los Angeles County Super. Ct. No. 24CJCF02649)

ORIGINAL PROCEEDINGS in prohibition. Charlaine Olmedo and Sam Ohta, Judges. Petition granted.

Spertus, Landes & Josephs, James W. Spertus, M. Anthony Brown, and Hans Allhoff for Petitioner.

Keker, Van Nest & Peters, Khari J. Tillery, Amrutha Dorai, Danika L. Kritter and Lauren Jung for Law School Professors as Amici Curiae on behalf of Petitioner.

No appearance for Respondent.

Rob Bonta, Attorney General, Lance E. Winters, Chief Assistant Attorney General, Susan Sullivan Pithey, Assistant

Attorney General, Zee Rodriguez and Charles Chung, Deputy Attorneys General, for Real Party in Interest.

Nathan J. Hochman, District Attorney (Los Angeles), and Matthew Brown, Deputy District Attorney, as Amicus Curiae on behalf of Real Party in Interest.

Real party in interest the People commenced a criminal prosecution against petitioner and defendant Diana Maria Teran (petitioner), alleging she improperly used information she learned when employed by the Los Angeles County Sheriff's Department during her later employment for another government agency, the Los Angeles County District Attorney's Office. We consider whether criminal prosecution for this alleged misconduct may be had under Penal Code section 502, subdivision (c)(2), which makes it a crime to "[k]nowingly access[ ] and without permission take[ ], cop[y], or make[ ] use of any data from a computer, computer system, or computer network."[1]

FACTUAL AND PROCEDURAL BACKGROUND

A felony complaint filed on April 24, 2024, charged petitioner with eleven violations of section 502, subdivision

---

[1] All further statutory references are to the Penal Code unless otherwise indicated.

(c)(2).[2] Each count concerns data relating to a different sheriff's deputy and alleges that "[o]n or about April 26, 2021, . . . Diana Maria Teran . . . did knowingly access and without permission take, copy, or make use of" data belonging to the Los Angeles County Sheriff's Department (LASD). An amended felony complaint filed on August 7, 2024, reduced the number of counts, and the total number of affected sheriff's deputies, to eight.

A. Preliminary Hearing Evidence

The following evidence was adduced at petitioner's preliminary hearing held between August 7 and August 20, 2024.

Petitioner worked as a constitutional policing advisor at LASD from 2015 to 2018. In that role, she was tasked with providing advice about the "best practices" for running LASD in a manner "consistent with . . . constitutionally supported polic[e] activities." She also assisted with efforts to ensure compliance with LASD's obligations pursuant to *Brady v. Maryland* (1963) 373 U.S. 83. To complete her work, petitioner reviewed and tracked complaints, investigations, and discipline involving deputies employed by LASD. Petitioner accessed this information in several ways. Petitioner utilized LASD's Performance Recording and Monitoring System (PRMS), a computer database that contained personnel information,

---

[2] That provision states that a public offense is committed if a person "[k]nowingly 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."

including information about complaints against sheriff's deputies, materials compiled during an investigation, findings of fact made by investigators, and documents stemming from civil service proceedings, such as court decisions following an appeal filed by a deputy or LASD. Petitioner reviewed similar information that LASD maintained in an excel spreadsheet tracking deputies' disciplinary proceedings. Additionally, other LASD employees emailed petitioner court documents from proceedings in which deputies were challenging civil service commission decisions. Petitioner also instructed her assistant to download files from PRMS and to share them with petitioner through email or a shared drive.

LASD had a Manual of Policy and Procedures (MPP) that contained rules concerning the protection of "official information maintained by the Department." Pursuant to the MPP, the "official business" of LASD was confidential, and "the content of any criminal record or other official information maintained by LASD either in manual files, microfilm records, or computerized systems shall be disclosed only to authorized persons." Authorized persons were prohibited from copying or using "any data or software, computer, computer system, or computer network" in order to "[w]rongfully control or obtain . . . data" or "[a]ssist in providing access to unauthorized persons to any data." Other law enforcement or government agencies could obtain information from LASD's official records only by request.

All LASD employees signed agreements that set forth how employees "should conduct themselves" with respect to data. LASD also trained employees before they could use the PRMS database and informed them that the records in the database were confidential. When logging into PRMS, users had to click to

accept a warning stating that misuse of the data contained within could result in prosecution. Petitioner left her position at LASD in November 2018.

In 2021, petitioner joined the Los Angeles District Attorney's Office (District Attorney). During the relevant time period, she was a special advisor in the Discovery Compliance Unit (DCU). The DCU maintains the District Attorney's databases that contain exculpatory and impeachment evidence that must be turned over to the defense under *Brady* as well as other information about law enforcement personnel that is not required to be disclosed.

On April 26, 2021, petitioner sent an email to another attorney in the DCU. Petitioner's email shared a digital folder titled "Writ Discipline Decisions" containing tentative and final superior court writ decisions that arose out of civil service proceedings involving numerous sheriff's deputies. The file name for each writ decision included the deputy's name, and most file names also indicated that the document was from a writ proceeding.

The particular sheriff's deputies and their involvement in these disciplinary matters did not appear in a search of major media outlets or in public records requests on the LASD website.[3] Writ decisions can be accessed by the public through the Los Angeles Superior Court website; however, those documents could not be located without searching based on both the name of a party and the court's case number. The metadata of the

---

[3] The amended felony complaint and trial court records refer the deputies as Deputy Does 1, 2, 4, 7, 8, and 9, and the parties continue that practice in their briefing in this court. For ease and clarity, we adopt this nomenclature.

documents that petitioner sent to her DCU colleague in 2021 regarding Deputy Doe 4 matched the metadata of those same documents that were located in an LASD shared drive folder created by the assistant that had worked for petitioner when she was at LASD. The metadata of the documents petitioner sent to her DCU colleague regarding Deputy Does 1, 2, and 7 matched the metadata of those same documents that had been emailed to petitioner during the time she was working at LASD. The documents that petitioner shared in the digital folder in 2021 lacked indicators that they had been obtained directly from the superior court docket: they were missing court filing stamps, signatures, and two-hole punches at the top of the page.

B. Order After Preliminary Hearing

On August 20, 2024, the trial court held petitioner to answer on six of the eight counts, those that concerned Deputy Does 1, 2, 4, 7, 8, and 9.

First, the trial court found there was sufficient evidence petitioner logged in to PRMS and accessed the Deputy Does' personnel records, which contained information about the complaint or discipline on the issue challenged in the writ proceeding. The court held that PRMS was the only method of acquiring the relevant data that met the statutory definition of "access," which is "to gain entry to, instruct, cause input to, cause output from, cause data processing with, or communicate with, the logical, arithmetical, or memory function resources to a computer, computer system, or computer network." (§ 502, subd. (b)(1).) The court concluded that there was a "logical inference of access," as any reasonable and competent person with petitioner's

job would have accessed the PRMS personnel records of these deputies to be thoroughly prepared. Next, the trial court found that, given LASD's policies regarding sharing information, there was evidence petitioner acted without LASD's permission when sending the April 26, 2021 email. The court then concluded that sending the court documents revealed the names of the Deputy Does obtained from PRMS (which are linked to "sensitive [and] confidential personnel records"), and that constituted "knowing use of the data accessed through PRMS."

The trial court declined to find that petitioner was subject to an exception under the statute for those acting within the scope of "lawful employment." (§ 502, subd. (h)(1).)

Finally, the court rejected an argument that the law was unconstitutionally vague as applied to petitioner, finding that PRMS alerted users of potential prosecution under section 502, which gave her fair warning before she accessed the data.

C. Section 995 Motion and Further Proceedings

On September 3, 2024, petitioner was arraigned on the information charging her with six counts. On September 30, 2024, she filed a motion to dismiss pursuant to section 995. On October 10, 2024, the trial court denied the motion. She filed a petition for writ of prohibition on October 24, 2024.

On November 6, 2024, the People filed a motion to strike three exhibits to the writ petition on the grounds that the exhibits had been sealed below. In response, we issued an order on November 8, 2024, proposing to unseal two of those exhibits and requesting briefing from the parties addressing the issue. Petitioner filed an opposition to the motion to strike on

November 18, 2024, arguing that all three of the exhibits were in the public domain and the information within had also been made public. No reply was filed.

After receiving preliminary opposition to the petition and a reply to the preliminary opposition from the parties, we issued an order to show cause why relief should not be granted on December 23, 2024. We now grant the petition and order the exhibits unsealed.

DISCUSSION

A. Standard of Review and Applicable Law

Section 995 requires an information to be set aside if the defendant "had been committed without reasonable or probable cause." (§ 995, subd. (a)(2)(B).) "Reasonable or probable cause . . . exists ' " 'if there is some rational ground for assuming the possibility that an offense has been committed and the [defendant] is guilty of it.' " ' " (*People v. Moyer* (2023) 94 Cal.App.5th 999, 1018.)

"In reviewing a trial court's ruling on a section 995 motion, we disregard the ruling of the trial court and directly review the magistrate's ruling." (*People v. Superior Court (Mendez)* (2022) 86 Cal.App.5th 268, 277.) "Insofar as the Penal Code section 995 motion rests on issues of statutory interpretation, our review is de novo." (*Lexin v. Superior Court* (2010) 47 Cal.4th 1050, 1072.)

"When we interpret a statute, '[o]ur fundamental task . . . 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 language permits more than one reasonable interpretation, courts may consider other aids, such as the statute's purpose, legislative history, and public policy.' [Citation.]" (*Sierra Club v. Superior Court* (2013) 57 Cal.4th 157, 165–166; see also *Commission on Peace Officer Standards & Training v. Superior Court* (2007) 42 Cal.4th 278, 290.)

B. The Parties' Factual and Legal Theories

The People's criminal prosecution of petitioner under section 502(c)(2) is based on the theory that petitioner "knowingly accessed the data from the Sheriff's Data Network" regarding the six deputies in the charged counts "during her LASD employment," and then, years later, on April 26, 2021, "made use of" that data. Although the felony complaint here, referencing the statutory language, alleges that petitioner "did knowingly access and without permission take, copy, or make use of data," the People concede they are not pursuing a theory of taking or copying.[4] Rather, the People attempt to show "use" of the data

[4] The magistrate found that any charges based on taking or copying of data would fall outside the three-year statute of limitations, because those acts would have occurred while petitioner still worked at LASD. The People explicitly concede

without permission, stating: "[e]ach step petitioner took – identifying the deputies from data on the Sheriff's Data Network, selecting documents pertaining to each, titling those document so that they revealed the deputies' names, and sending the curated group of names and documents to [her DCU colleague] – falls under the dictionary definition of " ' to make use of.' " " As best we can understand, the People appear to advance a theory that petitioner made use of data by sharing with her colleague the copies of the court documents, as well as a theory that she made use of data by disclosing the names of deputies to her DCU colleague in the titles selected for each document (regardless of the documents' contents).

To fit this conduct within the meaning of section 502(c)(2), the People urge us to adopt an interpretation of the statute's prohibition against "use" of "data" "without permission" that recognizes essentially no limits on the nature of the data at issue. According to the People, the data need not be confidential, proprietary, or sensitive in any respect, and extends to purely public records. The People likewise see no practical limits on what might constitute "use" "without permission." For example, if years after leaving a job at a prior employer, an employee recalls by memory some information learned in an email from that employer, and shares it with her new employer, sharing that recollection would meet the definition of "use" without permission.[5] So long as a prosecutor can establish that a

---

this on appeal with respect to taking, and implicitly by not raising any issue with respect to copying.

[5] As relevant here, the People take the position that it is not even necessary to show that petitioner downloaded or saved

potential defendant learned the information from data on a computer, computer system, or computer network of another individual, business, or government agency, and later revealed something about that information without permission, the People argue the conduct is criminal, subject only to a prosecutor's discretion as to whether to file charges.[6]

Petitioner counters with a series of arguments attacking both the legal and factual bases for the prosecution; petitioner and Amicus Curiae Law School Professors also find the People's position constitutionally problematic, given petitioner's role at the DCU to ensure her own, and the District Attorney's, compliance with their constitutional obligations relating to *Brady* material. As we conclude that section 502(c)(2) does not make criminal the acts alleged in this case, we do not reach petitioner's arguments that the evidence was insufficient to establish that petitioner accessed confidential information and that petitioner is exempt from prosecution pursuant to section 502(h)(1). Our view of the proper scope of section 502(c)(2) also avoids the need to decide this case on constitutional grounds.

---

any documents from LASD and later used them, as anything she remembered from having seen it on a computer display at LASD could form the basis for a prosecution.

[6] At oral argument, the People took the position that under their construction of section 502(c)(2), petitioner's provision of copies of the court documents at issue here to her own lawyers to prepare her defense would constitute a separate violation of the statute, although she might have constitutional defenses against such charges, such as "necessity."

C. Analysis

1. The relevant statutory language: Use of data without permission

We accept that the plain language of section 502 includes an extremely broad definition of "data."[7] The statutory definition does not include any express requirements limiting the reach of the overall statute to non-public, confidential, or proprietary information; it does not limit data to information that is unique and possessed only by a single entity, but extends to information that is duplicative of that possessed by other entities; and it does not require that the entity whose computer is at issue have some legal ownership interest in the data itself. The breadth of this definition of data makes sense within the context of the overall statute: section 502 criminalizes a diverse range of conduct involving computer systems and data, prohibiting, among other things, altering, damaging, deleting, or destroying data without permission. (§ 502, subds. (c)(1), (4).) While the particular facts of a given case might raise questions about the statute's reach based on the nature of the data at issue, the application of section 502 to criminalize destructive conduct appears to come squarely within a central aspect of the Legislature's stated intent, to

---

[7] Section 502, subdivision (b)(8) states: " 'Data' means a representation of information, knowledge, facts, concepts, computer software, or 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."

protect computers systems and data against "tampering, interference, [and] damage." (§ 502, subd. (a).)

In this case, however, we are confronted with how the term "data" should be understood in the context of the particular provision of section 502 that criminalizes its "use" "without permission." (§ 502, subd. (c)(2).) The term "use" is not defined in the statute, nor does the statute include any language to explain the permission necessary for a given use of data. But the requirement that an individual obtain permission for the use of data that resides on an entity's computer can only be reasonably understood to apply to situations where the entity has some dominion over, or right to control, the uses made of that data.

There is an ambiguity created in the statutory language from trying to give full effect to both the broad definition of "data" and the requirement of permission: it would seem anomalous to read the statute to impose criminal sanctions on an individual for failing to obtain permission to use a document that is fully available from a public source just because the individual accessed an identical copy of the document from an entity's computer. Given the lack of clarity in how the plain text of the statute might apply in such a circumstance, we next turn to the legislative history and statutory purposes to determine whether an interpretation of section 502(c)(2) that would extend criminal liability to the making use of purely public documents, such as the court rulings at issue here, is consistent with legislative intent.

2. Legislative history and statutory purposes

The legislative history behind section 502 indicates that the Legislature intended this statute to prohibit acts that would qualify as hacking of or tampering with computers and data. Section 502 was first created in 1979 because "no statute specifically proscribes fraud committed by means of computer, or prohibits the alteration or destruction of computers or computer programs." (Sen. Com. on Judiciary, Analysis of Sen. Bill No. 66 (1979-1980 Reg. Sess.) as amended Apr. 23, 1979, p. 1.) There was concern that "[s]abotage of a computer could seriously disrupt business or government operations." (Assem. Com. on Crim. Justice, Analysis of Sen. Bill No. 66 (1979-1980 Reg. Sess.) as amended Jun. 19, 1979, p. 1.) The stated goal of this new legislation was to tackle computer "misuse," like the "manipulation resulting in the payment of money not owed" or the "concealment of embezzlement." (*Ibid.*) When the original statute was repealed and replaced in 1987, that concern remained at the forefront. The law was changed in order "to provide for increased penalties for computer 'hackers' and to provide standardized definitions of terms." (Assem. Com. on Pub. Safety, Analysis of Sen. Bill No. 225 (1987-1988 Reg. Sess.) as amended Sept. 8, 1987, p. 2.) The Legislature cited the fact that as of June 1984, 25 percent of America's largest companies suffered annual losses of between $145 and $730 million due to computer crime. (*Ibid.*)

This targeted purpose is reflected in the statement of legislative intent added to section 502 at that time, which remains part of the statute today. Section 502, subdivision (a)

reads: "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. The Legislature finds and declares that the proliferation of computer technology has resulted in a concomitant proliferation of computer crime and other forms of unauthorized access to computers, computer systems, and computer data. [¶] The Legislature further finds and declares that *protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data* is vital to the protection of the privacy of individuals as well as to the well-being of financial institutions, business concerns, governmental agencies, and others within this state that lawfully utilize those computers, computer systems, and data." (Emphasis added.)[8]

---

[8] In 1999, the Legislature made further amendments to section 502 to close a potential loophole in the statute that had risked allowing " ' "disaffected employees to maliciously tamper with a company's database . . . ." ' (Assem. Com. on Public Safety, Rep. on Assem. Bill No. 451 (1999–2000 Reg. Sess.) as amended Mar. 24, 1999, p. 6; Sen. Com. on Public Safety, Rep. on Assem. Bill No. 451 (1999-2000 Reg. Sess.) as amended Apr. 15, 1999, p. 9 [same].)" (*People v. Childs* (2013) 220 Cal.App.4th 1079, 1103.) The Legislature discussed a situation in which "an employee's job involves modifying or deleting files from a computer and that employee decides to delete an entire database out of malice." The inclusion of a new definition of "scope of employment" prevented malicious employees from victimizing their employers and then "avoid[ing] prosecution by claiming the deletion of files was within the scope of their employment." (See

We conclude from this history and statement of intent that the central concerns that compelled the Legislature to address computer crime were focused on conduct such as hacking into and tampering with computer systems and data, and the disruptions and costs of such conduct to the business of public and private entities. While we recognize that the statute includes, in section 502(c)(2), criminal penalties for the unauthorized taking, copying, and use of data, neither the legislative history nor statement of legislative intent identify the secondary use of materials obtained from an entity's computer system as a principal concern of the Legislature.

3. Reasonable construction of section 502(c)(2)

Recognizing that neither the plain language of the statute nor the legislative history and statement of purpose provide definitive guidance as to how to implement section 502(c)(2) in a circumstance involving publicly available documents, we next consider the consequences of the parties' differing interpretations, with the aim of adopting a construction that comports with the legislative intent and avoids unreasonable and arbitrary results. (See *Commission on Peace Officer Standards & Training v. Superior Court*, *supra*, 42 Cal.4th at p. 290.)

Referring to the language of section 502(c)(2), the People emphasize that the data here was "from" LASD's computer system, and offer an interpretation of section 502 that makes the

---

Assem. Com. on Public Safety, Rep. on Assem. Bill No. 451 (1999–2000 Reg. Sess.) as amended Mar. 24, 1999, p. 6; Sen. Com. on Public Safety, Rep. on Assem. Bill No. 451 (1999-2000 Reg. Sess.) as amended Apr. 15, 1999, p. 9 [same].)

location from which an individual obtains documents largely dispositive, while ignoring the public nature of the documents' contents. More specifically, the People contend that imposition of criminal liability "does not require that the data be confidential"; rather, what appears significant to the People is the mere fact that data is stored on a computer system and also that the entity who owns the computer system treats its data as confidential. Here, the People emphasize that LASD included warnings to persons accessing data on LASD's system that unauthorized use of the data was punishable under section 502. The People interpret section 502(c)(2) to effectively operate as a non-disclosure agreement backed by criminal penalties; absent permission, it is a crime for an employee to share with another party anything learned from computer data, whether it be in a database, an email communication, or otherwise.

We reject the People's attempt to construe section 502(c)(2) in this manner. First, we note that the People's position opens the door to arbitrary application of criminal liability. When pressed at argument about the lack of limits on the range of prosecutions that could be brought against individuals for sharing data that was purely public in nature, the People's consistent response was that although prosecutors could, they likely would not exercise their discretion to bring many such cases, or they could file cases as misdemeanor prosecutions. We draw a different conclusion: that the Legislature never intended this statute – which is principally aimed at computer hacking and tampering – to be used to criminally prosecute disclosure of purely public information that happened to be stored on a computer. Further, to the extent the People suggest the particular internal policies and practices of the computer owner –

e.g., mandating that employees abide by confidentiality provisions and restrictions on use or sharing of data, or giving warnings to persons accessing data about the possibility of criminal liability under section 502 – can transform the use of purely public data into something that can be prosecuted, we disagree. If the viability of criminal prosecutions under section 502(c)(2) turns on the entity's policies and warnings, there will be additional arbitrariness in criminal prosecutions across different public and private enterprises.[9]

Second, the People's construction of section 502(c)(2) is unreasonable in light of the purely public nature of the court records at issue in this case, even recognizing that the documents concern disciplinary proceedings involving peace officers. These court documents convey nothing that a member of the public could not learn by sitting in a courtroom attending the court proceedings or reviewing publicly available information from the court's docket and files. In *Pasadena Police Officers Assn. v. Superior Court* (2015) 240 Cal.App.4th 268, the court addressed California Public Records Act requests for an independent consultant's report reviewing the Pasadena Police Department's policies after an officer-involved shooting. The police officers and their union sought to enjoin disclosure of the full report, claiming that at least portions of it were exempted from disclosure because

---

[9] Public and private employers already have various means to prevent and redress violations of their policies regarding the unauthorized disclosure of their data by employees and former employees, including through civil litigation. We are confronted with a different question: whether the Legislature intended to provide for the People to address the unauthorized disclosure of purely public information (even if it was in violation of an employer's policies) by bringing a criminal prosecution.

they constituted confidential personnel material. The appellate court found that the police officers' revelation of certain information in court documents in a different case did not constitute waiver as to portions of the report that contained the same information. Yet in discussing the court documents (which included excerpts of officer deposition testimony), the appellate court observed that the "deposition testimony was given voluntarily, none of the transcripts was filed under seal and the officers chose not to shield their testimony or submissions or to seek a protective order." (*Id.* at p. 293, fn. omitted.) The court further stated that " ' "Court records are public records, available to the public in general . . . ." ' " and noted that the court records had been publicly available for well over a year. (*Ibid.*) The documents at issue here are years-old court records and there exists no evidence that any efforts had been made to shield either these documents or the information contained in them.

Nor do we credit as important the People's contention that LASD's decision to store court records of this kind in personnel or investigative files matters. The placement of public records in confidential personnel files does not transform them into confidential records. In the context of a case involving a request pursuant to the California Public Records Act, the California Supreme Court held that the determination of whether a document is confidential and shielded from disclosure under the statute is not made based on its location, but on its content. (*Commission on Peace Officer Standards & Training v. Superior Court*, *supra*, 42 Cal.4th at pp. 290–291.) To apply the law otherwise "would lead to arbitrary and anomalous results," like a newspaper article being deemed confidential by being placed into a police officer's personnel file. (*Id.* at p. 290.) It was held that

the Legislature could not have intended to permit the shielding of public records simply by placing them in a confidential personnel file. (*Id.* at p. 291.) Similarly, here we do not believe the Legislature intended to allow for criminal prosecution of an individual who shares a public court document just because the document had been stored as data on, and then retrieved by the individual from, LASD's PRMS. The placement of a public record in a particular file on a computer database does not transform a purely public court record into one over which a criminal prosecution then becomes possible when someone with computer access uses the document without permission of the owner of the computer.[10]

---

[10] Given our construction of the statute, we need not reach whether interpreting section 502 to permit prosecution for sharing public court records is discordant with constitutional law protecting the public's right to make use of such records. We note, however, that "the First Amendment provides a right of access to ordinary civil trials and proceedings." (*NBC Subsidiary (KNBC-TV), Inc. v. Superior Court* (1999) 20 Cal.4th 1178, 1212.) Article I, section 2 of the California Constitution similarly provides "broad access rights to judicial hearings and records." (*Copley Press, Inc. v. Superior Court* (1992) 6 Cal.App.4th 106, 111.) "[T]he public has an interest, in *all* civil cases, in observing and assessing the performance of its public judicial system, and that interest strongly supports a general right of access in ordinary civil cases." (*NBC Subsidiary, supra*, at p. 1210.) "Open court records safeguard against unbridled judicial power, thereby fostering community respect for the rule of law." (*In re Marriage of Nicholas* (2010) 186 Cal.App.4th 1566, 1575.) "If public court business is conducted in private, it becomes impossible to expose corruption, incompetence, inefficiency, prejudice, and favoritism. For this reason traditional Anglo-American jurisprudence

Finally, we reject the People's contention that petitioner did more than share purely public documents and information by selecting which deputies' writ decisions to share and titling each document to include the name of the deputy who was a party to the particular court proceeding. According to the People, this connected these particular deputies to discipline, which was confidential personnel information. The name of each deputy appears on the face of the corresponding court record, and any effort to describe the name of the document as conveying something more, or different than the court record, is entirely artificial. The only reasonable understanding of the information conveyed is that the name relates to the person discussed in the purely public court record, not some additional non-public information.

We conclude from the statutory language, and in particular the requirement that only use without permission may be prosecuted, the legislative history and statement of intent, and the arbitrary and unreasonable consequences that flow from the People's unconstrained reading of the statute, that section 502(c)(2) does not apply in circumstances where, as here, only purely public court records have been shared.

---

distrusts secrecy in judicial proceedings and favors a policy of maximum public access to proceedings and records of judicial tribunals." (*Estate of Hearst* (1977) 67 Cal.App.3d 777, 784.) Moreover, article I, section 3(b)(2) of the California Constitution states that "[a] statute, court rule, or other authority, including those in effect on the effective date of this subdivision, shall be broadly construed if it furthers the people's right of access, and narrowly construed if it limits the right of access."

D. Three Exhibits to the Petition Should be Unsealed

"In determining whether to unseal a record, the court must consider the matters addressed in rule 2.550(c)-(e)." (Cal. Rules of Court, rule 8.46(f)(5).)

California Rules of Court, Rule 2.550(c) provides that unless confidentiality is required by law, court records are presumed to be open. Rule 2.550(d) provides that a court may order a record sealed only upon making express findings that: "(1) There exists an overriding interest that overcomes the right of public access to the record; [¶] (2) The overriding interest supports sealing the record; [¶] (3) A substantial probability exists that the overriding interest will be prejudiced if the record is not sealed; [¶] (4) The proposed sealing is narrowly tailored; and [¶] (5) No less restrictive means exist to achieve the overriding interest." Rule 2.550(e) discusses the required content of a sealing order.

The exhibits at issue—Exhibits D33, D34, and D49—were sealed after being introduced at the preliminary hearing. They were ordered sealed because they referenced the Deputy Does' names and could be linked to other sealed exhibits that contained confidential information.

D33 and D34 are news articles from 2010 and 2013, respectively. D49 is made up of Internal Affairs Bureau investigation materials that were put on LASD's website.

On August 20, 2024, eight exhibits, court documents from writ proceedings involving the Deputy Does, were ordered unsealed. The unsealed exhibits name the Deputy Does and discuss details of their discipline. D34 and D49 describe the discipline that is discussed in two of those unsealed exhibits.

Further, the deputy names were published in the *Los Angeles Times* in September 2024.

Given that the exhibits have been made publicly available and that the information within them has also been made public, we find that unsealing the exhibits is appropriate. (See *H.B. Fuller Co. v. Doe* (2007) 151 Cal.App.4th 879, 898 ["there is no justification for sealing records that contain only facts already known or available to the public"]; *McNair v. National Collegiate Athletic Assn.* (2015) 234 Cal.App.4th 25, 34 [declining to seal an NCAA report that identified the plaintiff, in part because "the public already knows that plaintiff is . . . named in [the report]"]; *Universal City Studios, Inc. v. Superior Court* (2003) 110 Cal.App.4th 1273, 1285–1286 [denying motion to seal financial data because it was publicly filed in another case].)

DISPOSITION

Let a peremptory writ of prohibition issue restraining respondent court from further proceedings other than dismissal pursuant to Penal Code section 995. Upon issuance of the remittitur, the temporary stay is vacated. Defense Exhibits D33, D34, and D49 presently under seal in this matter shall be unsealed.

CERTIFIED FOR PUBLICATION.

MOOR, J.

WE CONCUR:

BAKER, Acting P. J.

KIM (D.), J.