SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF LOS ANGELES

PEOPLE OF THE SATE OF CALIFORNIA, Plaintiff V. DIANA MARIA TERAN, Defendants.	24CJCF02649 STATEMENT OF DECISION

I. INTRODUCTION

This case involves a high-ranking prosecutor in the Los Angeles County District Attorney's Office named Diana Maria Teran (Defendant) charged with violating Penal Code section 502, subd. (c)(2). The Defendant previously worked as a Constitutional Policing Advisor for the Los Angeles County Sheriff's Department (Sheriff) from 2015 to 2018.

This case is brought by the Attorney General Office for the State of California (People).

The People filed the original complaint on April 24, 2024.

The original complaint contained 11 counts all alleging a violation of Penal Code section 502, sub. (c)(2) naming the Los Angeles County Sheriff's deputies involved as Deputy Does 1 through 11 to preserve their alleged right to confidentiality under state law.

The substance of the counts in the complaint states:

> On or about April 26, 2021, in the County of Los Angeles, the crime of ACCESSING AND USING COMPUTER DATA WITHOUT PERMISSION in violation of Penal Code section 502 (c)(2), a felony was committed by Diana Maria Teran who did knowingly access and without permission take, copy, or make use of data from a computer, computer system, or computer network

concerning SHERRIF'S DEPUTY DOE and belonging to the LOS ANGELES COUNTY SHERRIF'S DEPARTMENT."

On August 7, 2024, the People filed an amended complaint moving to dismiss Counts 6, 10, and 11.

On August 8, 2024, the Defendant was re-arraigned on the amended complaint which dismissed Counts 6, 10, and 11.

The defendant again entered a not guilty plea to the remaining counts.

This court heard the preliminary hearing which began on August 8, 2024, lasting until August 13, 2024.

The Defendant and the People have filed closing summation briefs which the court has considered.

II. APPLICABLE LAWS

A. Charged Offense

The eight counts consist of one identical charge of violating Penal Code section 502, subd. (c)(2)[1]. This code section states as follows:

> Except as provided in subdivision (h), any person who commits any of the following acts is guilty of a public offense: 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.

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

The California Legislature passed this code section which the governor signed into law in 1987. While available for use by state prosecutors for the past 37 years, only one published opinion by the Court of Appeal exists on the application of subdivision (c) paragraph (2) entitled *People v. Hawkins* (2002) 98 Cal.App.4th 1428 (*Hawkins*). The facts in *Hawkins* are dissimilar to our case and therefore not very helpful as a legal guide. However, *Hawkins* instructs that the *mens rea* for this offense is the word "knowingly" which applies both to the "access" as well as to the "takes, copies, or makes use" components of (2). Based on *Hawkins*, the elements of this offense are as follows:

1. A person knowingly accessed a computer, computer system, or computer network; and
2. That person, without permission, knowingly took, copied, or made use of any data from a computer, computer system, or computer network.

The Court and counsel's research have not turned up any decisional law applying section 502, subd. (c)(2) to facts like this prosecution. To that extent, we are in uncharted territory.

B. Rules Related to the Preliminary Hearing

A preliminary hearing is not a trial but is considered an abbreviated hearing. *People v. Slaughter* (1984) 35 Cal.3d 629. At the preliminary hearing, the prosecutor is required to present evidence to a judicial officer who serves as magistrate to make a legal determination whether there is sufficient evidence to hold a defendant for trial in a felony case. In a preliminary hearing, "probable cause is shown if a man of ordinary caution or prudence would be led to believe and conscientiously entertain a strong suspicion of the guilt of the accused." (*Rideout v. Superior Court of Santa Clara County* (1967) 67 Cal.2d 471, 474.

The standard applied is probable cause, the same standard used to execute a warrant, or for law enforcement to arrest an individual for an alleged crime. This is a legal determination, not a factual one. The highest standard of law – beyond a reasonable doubt – is not implicated here as the purpose of the preliminary hearing is not factual to determine whether the Defendant is guilty of a crime.

C. Prosecutor's Duty Under Brady v. Maryland

The underlying facts of this case involve the prosecutor's duty to disclose exculpatory or impeachment evidence to criminal defendants.

In 1963, the United States Supreme Court published *Brady v. Maryland* (1963) 373 U.S. 83 (*Brady*) which established that the suppression by the prosecution of evidence favorable to an accused upon request violates due process where the evidence is material either to guilt or to punishment, irrespective of the good faith or bad faith of the prosecution. (*Id.* at 87.)

Over the years, *Brady* - enshrined in the Due Process Clause of the Fifth Amendment applicable to the states through the Fourteenth Amendment of the federal Constitution has received additional explanations through published decisional laws both at the state and federal levels.

Izazaga v. Superior Court (1991) 54 Cal.3d 356 (*Izazaga*) dealt with a defense challenge to the informal discovery process in criminal cases under Proposition 115. In the case, the petitioner asserted that the new discovery chapter violated the due process clause because the new statute did not require the prosecution to disclose *Brady* evidence. To this challenge, the *Izazaga* Court explained that:

> "The prosecutor's duties of disclosure under the due process clause are wholly independent of any statutory scheme of reciprocal discovery. The due process requirements are self-executing and need no statutory support to be effective.

> Such obligations exist whether or not the state has adopted a reciprocal discovery statute. Furthermore, if a statutory discovery scheme exists, these due process requirements operate outside such a scheme. The prosecutor is obligated to disclose such evidence voluntarily, whether or not the defendant makes a request for discovery." (*Id.* at 378.)

In *Kyles v. Whitley* (1995) 514 U.S. 419 (*Kyles*), the high court reasoned, "the individual prosecutor has a duty to learn of any favorable evidence known to the others acting on the government's behalf in the case, including the police." (*Id.* at 437.) Generally referred to as the "prosecution team," a prosecutor is not permitted to claim he or she did not know of the existence of the evidence that meets *Brady* because the police never shared it. As members of the prosecution team, both are held accountable for the failure to disclose evidence that meets the *Brady* rule with a possible sanction of a reversal of the conviction if the accused can show materiality, which is defined as a reasonable probability, had the evidence been disclosed, the result of the trial would have been different. (*People v. Zambrano* (2007) 41 Cal.4th 1082, 1133.)

In *People v. Salazar* (2005) 35 Cal.4th 1031, the California Supreme Court summarized *Brady* as follows: "In *Brady*, the United States Supreme Court held "that the suppression by the prosecution of evidence favorable to an accused upon request violates due process where the evidence is material either to guilt or to punishment, irrespective of the good faith or bad faith of the prosecution." [Citation.] The high court has since held that the duty to disclose such evidence exists even though there has been no request by the accused [citation omitted], that the duty encompasses impeachment evidence as well as exculpatory evidence [citation omitted], and that the duty extends even to evidence known only to police investigators and not to the prosecutor. [Citation.]. Such evidence is material "" 'if there is a reasonable probability that, had the evidence been disclosed to the defense, the result of the proceeding would have been different.' "" [Citation.] In order to comply with *Brady*, therefore, ""the individual prosecutor has a duty to

learn of any favorable evidence known to the others acting on the government's behalf in the case, including the police."" [Citation.]" (*Id.* at 1042.)

D. Peace Officers' Right to Confidentiality of Personnel Records

Peace officers' duties in the field are sometimes dangerous, and their status as peace officers may pose risks to their safety, including those of family members, if personal information was made open to the public. On the other hand, as discussed, *ante*, law enforcement as part of the prosecution team must disclose exculpatory or impeachment evidence. Addressing these competing interests, the California Legislature codified several laws balancing the need to protect peace officers from risk to their safety by rendering their personnel records confidential while providing access to information through a procedure commonly referred to as a "Pitchess Motion."

In *People v. Mooc* (2001) 26 Cal.4th 1216, the California Supreme Court explained the interplay between several provisions in the penal and evidence codes when a Pitchess Motion is filed. The Supreme Court noted, "In *Pitchess v. Superior Court* [citation omitted], we recognized that a criminal defendant may, in some circumstances, compel the discovery of evidence in the arresting law enforcement officer's personnel file that is relevant to the defendant's ability to defend against a criminal charge. In 1978, the California Legislature codified the privileges and procedures surrounding what had come to be known as 'Pitchess motions' ... through the enactment of … sections 832.7 and 832.8 and Evidence Code sections 1043 through 1045." (*Id.* at 1219.)

Section 832.7, subd. (a) provides in pertinent part, "Except as provided in subdivision (b), the personnel records of peace officers and custodial officers and records maintained by a state or local agency pursuant to Section 832.5, or information obtained from these records, are

confidential and shall not be disclosed in any criminal or civil proceeding except by discovery pursuant to Sections 1043 and 1046 of the Evidence Code."

In *Copley Press, Inc. v. Superior Court* (2006) 39 Cal.4th 1272 (*Copley*), the California Supreme Court explained that section 832.7, subd. (a) "applies to two categories of records. The first is "personnel records" which is defined by section 832.8." (*Id.* at 1238.) The second category are '"records maintained by any state or local agency pursuant to [s]ection 832.5."' (*Ibid.*)

Section 832.8, subd. (a) defines "personnel records" as "any file maintained under that individual's name by his or her employing agency" and containing records that relate to six categories of circumstances which are: (1) Personal data, including marital status, family members, educational and employment history, home addresses, or similar information; (2) Medical history; (3) Election of employee benefits; (4) Employee advancement, appraisal, or discipline; (5) Complaints, or investigations of complaints, concerning an event or transaction in which he or she participated, or which he or she perceived, and pertaining to the manner in which he or she performed his or her duties; and, (6) Any other information the disclosure of which would constitute an unwarranted invasion of personal privacy. (See Pen. Code § 832.7, subd. (a)(1)-(6).) It appears, matters related to employer discipline can fit under category 4 or 5.

Despite the definition provided under section 832.8, subd. (a), what constitutes protected information has undergone some ebb and flow, some expansion, and some restriction.

First, in *Copley*, the California Supreme Court determined that records of San Diego County's Civil Service Commission constituted protected records under 832.7(a) and 832.8 even though the commission was not the peace officer's actual employer. (*Copley Press, Inc. v. Superior Court, supra*, 39 Cal.4th at p. 1288.) In concluding that the commission was a part of the employing agency, the California Supreme Court said, "because the Commission, a department of the County, has been designated to provide the appeal that the officer's employer is required by law to provide in connection with taking punitive action, it is reasonable to conclude that for

purposes of applying the relevant statutes in this case, the Commission is functioning as part of "'the employing agency'" and that any file it maintains regarding a peace officer's disciplinary appeal constitutes a file "'maintained ... by [the officer's] employing agency'" within the meaning of section 832.8." (*Ibid.*)

Next, in *Commission on Peace Officer Standards and Training v. Superior Court* (2008) 42 Cal.4th 278 (*POST*) the California Supreme Court held that an "officers' names, employing departments, and dates of employment when not sought together with any of the personal or sensitive information ... [are] not '"personal data"' within the meaning of section 832.8, subdivision (a)(1). (*Id.* at 299.) For this holding, the California Supreme Court relied on the rationale that in adopting sections 832.7 and 832.8, the Legislature was not concerned with making the identities of peace officers confidential based on employment status alone but instead on "linking a named officer to the private or sensitive information listed in section 832.8." (*Id.* at 295.) Thus, when an officer's name is linked with the specified types of information concerning a named officer as defined under section 832.8, subd. (a) (1)-(6), the name is confidential. For the opposite proposition, when an officer's name is not linked with confidential personnel records, it is not confidential.

The Court's reasoning in *POST* also dealt with section 832.7, sub. (a)'s phrase "information obtained from these records." The Court said, "[w]e consider it unlikely the Legislature intended to render documents confidential based on their location, rather than their content." (*Id.* at 291.) As discussed, *ante*, the Court focused on linking non-confidential information, here, the name of the peace officer, to the sensitive confidential information contained in the personnel file as defined under section 832.8, subd. (a).

The California Supreme Court took on another case to explain when the name of peace officers is not confidential in *Long beach Police Officers Association v. City of Long Beach* (2014) 59 Cal.4th 59 (*Long Beach*). Unlike *POST* which involved a public records request made

to the Commission on Peace Officer Standards and Training by the media unrelated to any incident of potential police misconduct. *Long Beach* dealt with a police shooting and killing of an intoxicated individual mistaken as brandishing a gun when he only possessed a garden hose spray nozzle with a pistol grip. (*Id.* at 64.)

In concluding that the names of the officers involved in the shooting were not confidential, the Court reasoned, "[a]lthough the *Pitchess* statutes limit public access to personnel records [citation omitted], including officer names if they are linked to information in personnel records [citation omitted], many records routinely maintained by law enforcement agencies are not personnel records. For example, the information contained in the initial incident reports of an on-duty shooting are typically not '"personnel records"' as that term is defined in Penal Code section 832.8. It may be true that such shootings are routinely investigated by the employing agency, resulting eventually in some sort of officer appraisal or discipline. But only the records generated in connection with that appraisal or discipline would come within the statutory definition of personnel records [citation omitted]. We do not read the phrase '"records relating to ... [¶] ... [¶] ... [e]mployee ... appraisal[ ] or discipline" [citation omitted] so broadly as to include every record that might be considered for purposes of an officer's appraisal or discipline, for such a broad reading of the statute would sweep virtually all law enforcement records into the protected category of '"personnel records"' [citation omitted.]" (*Id.* at pp. 71-72.)

Long Beach left some room for wiggle. First, it seems certain, after a peace officer shoots an unarmed individual that the employing law enforcement agency would conduct an internal affairs investigation as to whether the shooting was justified. In that sense, the name of the peace officer may arguably be linked to a personnel record as defined under section 832.8, subd. (a). Also, the Court did not discuss timing as to whether the request for the name must precede any internal affairs investigation so that once the law enforcement agency initiates the internal affairs investigation, the name would be linked and confidential. Instead, the Court reasoned that, "[i]t ...

appears that the Legislature [drew] a distinction between (1) records of factual information about an incident (which generally must be disclosed) and (2) records generated as part of an internal investigation of an officer in connection with the incident (which generally are confidential)." (*Id.* at 72.) By this explanation, the Court appears to suggest the existence of a non-confidential report (such as an initial incident report) stands separate from a parallel internal affairs report generated by the law enforcement agency. This area appears somewhat muddled.

E. Court Proceedings Related to the Category Under Section 832.8, subd. (a)

A Los Angeles County employee, dissatisfied with the result of the Los Angeles County Civil Service Commission's administrative appeal, may seek a writ of mandamus in the superior court[2]. (See Code Civ. Pro., § 1094.5) When an employee takes such an action, a question arises on whether the employee has waived the right of confidentiality in the personnel file on the same subject.

This was answered in *Pasadena Police Officers Association v. Superior Court* (2015) 240 Cal.App.4th 268 (*Pasadena*). The *Pasadena* Court said, "The fact that information in an officer's personnel records may also be found in an unprotected source does not impact the confidentiality of the personnel records themselves. The '"Pitchess statutes create a privilege for all information in peace officers' personnel files without regard to information found elsewhere."' [Citation.] The purpose and policy of the Pitchess statutes mandates that waiver of the privilege must be express. This is true even where, as here, the officers themselves placed the information in the public domain. ¶ Absent an express waiver of the privilege with respect to the confidential personnel information found in the Report, the officers retain *Pitchess* protections as to that information, even if the information is the same as or similar to information available elsewhere in the public domain." (*Id.* at 294.)

[2] A dissatisfied county department employer may also file a request for a writ of mandamus with the superior court which may alter the analysis on confidentiality.

Pasadena suggests, therefore, that while the information in the public court document is not confidential, the peace officer – unless expressly waived – retains confidentiality in the information contained in the personnel records.

F. Interplay Between Brady and Peace Officer's Right of Confidentiality

Tension exists between a criminal defendant's right to impeachment evidence under *Brady* and the right of the peace officers to their right of confidentiality in their personnel record on information that may impeach their credibility as witnesses. Not every complaint or discipline falls under *Brady*. Another source of tension is between law enforcement and the prosecutor who, as explained in *Kyles*, is obligated to provide *Brady* material to the defense, even if potentially unknown to the prosecutor but known to law enforcement, such as information contained in personnel files.

The California Supreme Court resolved some of this tension in *Association for Los Angeles Deputy Sheriffs v. Superior Court* (2019) 8 Cal 5th 28 (*ALADS*). *ALADS* centered on the Los Angeles County Sheriff's policy of providing a list of deputies whose personnel files may contain allegations of misconduct involving moral turpitude or other bad acts that allegedly met the requirements of *Brady* as exonerating or impeachment evidence. (*Id.* at 36.)

The Court in *ALADS* engaged in the following syllogism:

(1) A prosecutor is obliged under *Brady* to disclose evidence favorable to the accused. (*Id.* at 36.)

(2) This duty includes impeachment evidence on law enforcement testimony. (*Ibid.*)

(3) This duty to disclose is required even if the prosecutor is unaware of its existence. (*Ibid.*)

(4) This duty carries an obligation for the prosecutor to learn of favorable evidence beyond his or her personal knowledge. (*Ibid.*)

(5) "The so-called Pitchess statutes, however, restrict a prosecutor's ability to learn of and disclose certain information regarding law enforcement officers [Citations.]" (*Ibid.*)

ALADS ultimately concluded that law enforcement agencies are permitted to create a *Brady* list and provide them to prosecutors. In reaching this conclusion, the Court explained, "it is hard to imagine that the term '"confidential"' would categorically forbid one employee of a custodian of records, tasked with maintaining personnel files, from sharing those records with another employee assigned to the same task. Put differently, deeming information '"confidential"' creates insiders (with whom information may be shared) and outsiders (with whom sharing information might be an impermissible disclosure). The text of the *Pitchess* statutes does not clearly indicate that prosecutors are outsiders, forbidden from receiving confidential *Brady* alerts." (*Id.* at 50.) Before providing this rationale, the Court also found that the *Brady* list contained confidential information. The Court reasoned, "The identities of officers on the *Brady* list constitute '"information obtained from"' '"the personnel records of peace officers."' [Citation.] The *Brady* list is a catalog of officers with a particular kind of discipline-related information in their personnel file. It was derived from information in those files. It follows that, barring the applicability of an exception, the *Pitchess* statutes render confidential the identities of officers on the *Brady* list. To hold otherwise would mean that section 832.7(a) affords the *Brady* list no protection at all." (*Id.* at 47.) To reiterate, the name of a peace officer obtained from the personnel file and linked to that file is confidential.

With this backdrop of the generally applicable laws, we move on to the analysis.

III. ANALYSIS

A. The People's Theory of Liability

The People's view of the facts supporting their theory of liability, as stated in open court on August 13, 2024, may be summarized as follows:

1. The Los Angeles County Sheriff's Department (Sheriff) owns a computer network called the "Sheriff Data Network" (SDN).
2. The Defendant worked as an employee for the Sheriff from 2015 to 2018 (Constitutional Policing Advisor – a high level position near the Sheriff in hierarchy) and used the SDN as an employee.
3. The Defendant accessed data in the SDN as a Constitutional Policing Advisor whose job was to oversee policing issues related to complaints and internal affairs which necessitated accessing various forms of data connected to sensitive personnel files.
4. As the Constitutional Policing Advisor, the Defendant knew the deputies who were subject to internal investigations from which she created a list.
5. This list of names is protected as they are linked to or derived from protected information.
6. When the Defendant left the Sheriff in 2018, she took data from the SDN as shown by the metadata on various pdf documents discovered during the investigation by the People.
7. The Defendant was hired by the Los Angeles County District Attorney in 2021 in another high-level position.
8. On April 26, 2021, the Defendant sent an email to Deputy District Attorney (DDA) Pamela Revel who was assigned to the Discovery Compliance Unit (DCU), a unit over which the Defendant supervised.

9. The DCU was responsible for maintaining a list of peace officers to comply with *Brady*.

10. The DCU maintained two lists: *Brady* and another called Officer Recurring Witness Information Tracking System (ORWITS).

11. The difference between the two is that the alleged misconduct for peace officers on the *Brady* list must meet the requirements of the *Brady* rule whereas the ORWITS list is for less egregious allegations of misconduct.

12. The email sent to DDA Revel contained numerous attachments.

13. The attachments included several court documents which related to writ proceedings under California Code of Civil Procedure, section 1094.5, a process to challenge the administrative decision of the Los Angeles County Civil Service Commission (Commission).

14. The attachments to the email sent to DDA Revel consisted of various deputy sheriffs who sought to challenge the decision of the Commission, including the eight Deputy Does for the eight counts on the amended complaint.

15. The Defendant knew she was using data taken from the SDN without permission because she was an employee who had to abide by the manual of policies and procedures who knew of the procedures and had signed an annual acceptable use policy required by the Sheriff.

16. The Defendant knew disseminating information derived from or linked to confidential information was impermissible because of a "splash screen" which appeared when a person logged into a specific component of the

SDN called Personnel Reporting Management System[3] (PRMS) which retains personnel records related to complaints and disciplines.

17. This splash screen warned that unauthorize use of PRMS could result in criminal prosecution for violating section 502 which had to be bypassed before accessing PRMS.

18. The Defendant knowingly used information belonging to the Sheriff because she is a sophisticated individual who would understand county policies and the ethical duties that would allow her to share certain information.

B. People's Theory Regarding the Breach of Confidentiality

This case turns on whether the Defendant breached the confidentiality of personnel records protected under section 832.7, subd. (a) and as defined under section 832.8, subd. (a) or section 832.5. This question relates to the "access" element of the charged offense.

In their closing summation brief, the People argues, "On April 26th 2021, the defendant sent an e-mail to DCU employee, deputy District Attorney Pamela Revel. The e-mail contained a shared folder that, if opened, contained a list of LASD deputy names who had been the subject of internal investigations of complaints and/or involving discipline. This list of names was compiled from the various forms of data that the defendant had accessed and taken from the sheriff's data network including the PRMS database, the tracker excel databases, e-mail attachments, and documents stored within the Sheriff's Data Network sent to her by Wang. "

The People do not argue that the court documents sent as attachment to DDA Revel which are the basis of this prosecution constitute personnel records as defined under section 832.8, subd. (a). These court documents do not fit under *Copley* because they (1) were not

[3] The People's summation brief refers to PRMS as Performance Recording Monitoring System – however, this is not the testimony on the name for the acronym by Detective Bernstein.

generated or created by the employing law enforcement agency for a specified reason under section 832.8, subd. (a), (2) were not created by an administrative appeal process like an appeal to a commission set up by local ordinances as an employer granted right, (3) are open to the public under California Rules of Court Rule 2.550 (c) with some exceptions that do not apply here, and (4) were created based on the voluntary act of the disaffected county employee who filed a request for a writ of mandamus with the court system pursuant to Code of Civil Procedure, section 1094.5.

Instead, the People rely on a theory based on a combination of two laws – first, on statutory language in section 832.7, subd. (a) ("information obtained from these records") and second, on decisional laws ("linking a named officer to the private or sensitive information listed in section 832.8"). *(Commission on Peace Officer Standards and Training, supra*, 42 Cal.4th at p. 295.)

Filtering this theory through the elements of the charged offense is helpful. Proving a violation of section 502, subd. (c)(2) requires showing: (1) A person knowingly accessed a computer, computer system, or computer network; and (2) That person, without permission, knowingly took, copied, or made use of any data from a computer, computer system, or computer network. Based on the statute of limitation under section 801[4], the People are limited to the "made use of data" part of element 2. Thus, the prosecution must show the Defendant knowingly accessed the Sheriff's computer, computer system, or computer network, and ***used data*** from that computer, computer system, or computer network, without the permission of the Sheriff.

---

[4] California Penal Code section 801 states, "Except as provided in Sections 799 and 800, prosecution for an offense punishable by imprisonment in the state prison or pursuant to subdivision (h) of Section 1170 shall be commenced within three years after commission of the offense.

In the instant case, the "data" relates to the email attachments the Defendant sent to DDA Revel on April 26, 2021. Within that email attachment, the data relied on by the People **is the name of the deputy sheriff attached** to the pdf documents.

The Defendant contends, she cannot be prosecuted for using court documents that do not belong to the Sheriff. The specific issue in this case, however, is not ownership of the document. Rather, it is whether the Defendant accessed the protected computer network owned and maintained by the Sheriff - as will be more fully explained below – and obtained the names linked to their personnel file as enumerated in the various counts.

C. Element 1 – Accessing the List of Names of Deputies as Data

As discussed, *ante*, names of peace officers are not confidential but becomes so if linked to sensitive confidential records. Names of the deputies involved in this case as a Deputy Doe, therefore, must be linked to sensitive information in each of their personnel records maintained by the Sheriff required by law.

Under this theory, to prove the first element of knowingly accessing a computer, a computer system, or computer network, the People must show that the Defendant accessed the personnel records in the computer network – the sensitive information – related to the writ document that was sent to DDA Revel. Evidence adduced at the preliminary hearing shows, the Sheriff maintains an umbrella network called SDN. Within SDN are additional compartments requiring a separate access through use of a name and password, including PRMS. Here, the People must show that the Defendant accessed Deputy Doe's personnel record which contained information about the complaint or discipline on the issue challenged in the writ proceeding in superior court. This is PRMS. Indeed, the People made a point by asking one of their witnesses, Detective Todd Bernstein, about the so-called "splash screen" which must be bypassed when a user logs in to PRMS which warns of prosecution for violating section 502 before the user is

permitted to access the sensitive personnel records. This is a point well made by the People. This is the specific part of the "computer, the computer system, or computer network" the People must show the Defendant accessed.

Merely showing that the Defendant had access to the various deputy's personnel records or evidence that the Defendant accessed any of the Deputy Doe's personnel records at some point in time does not prove this element. This is because the "access" and the "use" element must relate to the same subject matter – here – the use of the deputy's name linked to the sensitive confidential record stored in PRMS as revealed to DDA Revel by attaching the writ document to the email.

To clarify further, the People are not required to prove that the writ document was placed into PRMS and that the Defendant acquired the writ document from PRMS. Instead, the evidence must show, the Defendant accessed the computer network – the PRMS – and obtained the protected information – the name of the Deputy Doe on a specific personnel record issue challenged by the writ process – which she allegedly improperly revealed by providing the writ document on that same subject. Therefore, a potential breach of confidentiality is not coequal with a violation of section 502, subd. (c)(2).

This is so because a deputy who is the subject of the writ document revealed to DDA Revel may claim his or her privilege was breached by the disclosure of the writ pdf linked to his or her confidential file without showing that the Defendant knowingly accessed PRMS.

The People suggest accessing the SDN is the computer network the People must show to prove element 1 on access. This court disagrees.

The following analysis may be helpful. The Legislature defined the term "access" in the statute. "'Access'" means 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 of a computer, computer system, or computer network." (See Pen. Code § 502, subd. (b)(1).) In

Chrisman v. City of Los Angeles (2007) 155 Cal.App.4th 29 (*Chrisman*), the Court of Appeal said, "[s]ection 502 defines '"access"' in terms redolent of '"hacking"' or breaking into a computer." (*Id.* at 34.) "One of the legislative purposes of Penal Code section 502 was 'to deter and punish ... browsers and hackers—outsiders who break into a computer system to obtain or alter the information contained there....' [Citation.]" (*People v. Gentry* (1991) 234 Cal.App.3d 131, 141, fn. 8.)

As the Constitutional Policing Advisor, based on email lodged as exhibits in this case, it is clear, the Defendant advised the Sheriff on matters related to outside writ litigation under Code of Civil Procedure, section 1094.5. The Sheriff and the deputy sheriff are on opposite sides with counsel representing both. It seems reasonable, counsel representing the Sheriff would send writ documents to the Constitutional Policing Advisor or others in the unit notifying them on the progress and outcome of the various writ proceedings. This type of communication sometimes probably occurred via email with attachments of the writ documents being litigated. These documents did not originate in Deputy Doe's personnel records. They are court records. This court cannot conceive such receipt of writ documents in pdf format from outside the Sheriff's network constitutes access as defined in section 502, subd. (b)(1) which is gaining entry to, instructing, causing input to, causing output from, causing data processing with, or communicating with, the logical, arithmetical, or memory function resources of a computer, computer system, or computer network, as required to be shown in a violation of section 502, subd. (c)(2).

1. Evidence of Access

To prove access, the People rely on circumstantial evidence. Neither Exhibit B (tracker spread sheet), Exhibit C (spreadsheet prepared by Detective Todd Bernstein) or the various emails exchanges during the Defendant's employment as the Constitutional Policing Advisor

directly shows access to PRMS connected to the personnel issue addressed in the writ proceeding.

Circumstantial evidence requires logical inferences. "An inference is a deduction of fact that may logically and reasonably be drawn from another fact or group of facts found or otherwise established in the action." (Evid. Code, § 600, subd. (b).) However, "[a] reasonable inference ... 'may not be based on suspicion alone, or on imagination, speculation, supposition, surmise, conjecture, or guess work. [¶] ... A finding of fact must be an inference drawn from evidence rather than ... a mere speculation as to probabilities without evidence.' [Citation.]" (*People v. Morris* (1988) 46 Cal.3d 1, 21)

a. Existence of Logical Inference Based on Evidence

This case is technical in nature and small details matter. After careful review of such details in the People's evidence, this court concludes logical inference based on circumstantial evidence exists as to Counts 1, 2, 4, 7, 8 and 9 on the issue of access. Here, it is important to remember, this court is not conducting a trial where, if two reasonable inferences exist, the trier of fact is required to adopt the one that points to innocence. (CALJIC 2.01.)

On Count 1, the logical inference of access is based on Exhibit D – the email with the attachment of the writ document (Exhibit E). The email was sent by Piro Ranasinghe to the Defendant. Mr. Ranasinghe is entitled a Legal Advisor in the Sheriff's Department. The content of the email shows the case involved a writ during the Defendant's tenure as the Constitutional Policing Advisor. It seems clear one of the big tasks of the Constitutional Policing Advisor was to keep the Sheriff and his assistants apprised on matters related to deputy discipline and results of outside litigation. In the email, there is some discussion concerning the issues handled in the writ proceeding. While the email does not specifically address whether the Defendant accessed Deputy Doe 1's PRMS personnel records, it is logical to conclude, on a writ proceeding

occurring when the Defendant was tasked with advising the Sheriff, any reasonable and competent advisor would have accessed Deputy Doe 1's personnel record to be thoroughly prepared.

On Count 2, the logical inference of access is based on Exhibit G – the email with two attachments of the writ documents (Exhibit H and Exhibit J). The email appears to have been sent from the Advocacy Unit of the Sheriff to the Defendant on two separate writs for Deputy Doe 2. Both writs, based on the dates on Exhibit H and Exhibit J, were matters pending during the Defendant's tenure as Constititonal Policing Advisor. The case numbers on Exhibit H and Exhibit J match the case numbers mentioned in the body of the email. Again, while the email does not specifically address whether the Defendant accessed Deputy Doe 2's PRMS personnel records, it is logical to conclude, on a current writ proceeding on which the Defendant was tasked with advising the Sheriff, any reasonable and competent advisor would have accessed Deputy Doe 2's personnel record to be thoroughly prepared.

On Count 4, the logical inference of access is based on Exhibit R – the chain email regarding Deputy Doe 4. The email chain shows the Defendant was a part of the discussion. Exhibit U is the document related to Exhibit R, although Exhibit U was not attached to the email. Correspondence between Exhibit R and Exhibit U is based on the content of the email and the unredacted version of the writ document. The content of the email shows Deputy Doe 4 was soon to return to work in March of 2015. This may have been close in time to when the Defendant began to serve as the Constitutional Policing Advisor. Again, it is logical to conclude, on a writ proceeding occurring when the Defendant was tasked with advising the Sheriff, any reasonable and competent advisor would have accessed Deputy Doe 4's personnel record to be thoroughly prepared.

On Count 7, the logical inference of access is based on Exhibit N – the chain email regarding Deputy Doe 7. The last email is the Defendant sending Lieutenant Jason Skeen an

attachment of Deputy Doe 7's writ. The body of the writ document shows the proceedings occurred during the Defendant's tenure as Constitutional Policing Advisor. The court's decision was to rescind the Sheriff's discipline. Again, it is logical to conclude, on a writ proceeding occurring when the Defendant was tasked with advising the Sheriff, any reasonable and competent advisor would have accessed Deputy Doe 7's personnel record to be thoroughly prepared.

On Counts 8 and 9, the logical inference of access is based on Exhibit Y – an email from the Advocacy Unit to, among others, the Defendant. The email references attachments for Deputy Doe 8 and Deputy Doe 9 by the names of both deputies. The attachments are not the writ documents sent to DDA Revel on April 26, 2021.

The email attachment for Deputy Doe 8 is Exhibit Z which is a Civil Service Commission generated document. The commission's document is confidential per *Copley*. This court has reviewed the unredacted commission document. The content of the commission generated document has been compared to the writ document sent to DDA Revel (Exhibit BBB). Exhibit Z and Exhibit BBB relate to the same subject matter. The commission document names the hearing officer. The content of Exhibit BBB mentions the hearing officer's name. It is the same individual. The writ proceeding for Deputy Doe 8 occurred during the time the Defendant served as the Constitutional Policing Advisor.

The email attachment for Deputy Doe 9 is Exhibit AA – a document generated by the Civil Service Commission. The commission's document is confidential per *Copley*. The commission's order on the underlying matter shows the nature of the issue. The content of the commission generated document has been compared to the writ document sent to DDA Revel (Exhibit DDD). The writ proceeding for Deputy Doe 8 occurred during the time the Defendant served as the Constitutional Policing Advisor.

As for Deputy Doe 8 and Deputy Doe 9, it is logical to conclude, on a writ proceeding occurring when the Defendant was tasked with advising the Sheriff, any reasonable and competent advisor would have accessed Deputy Doe 8 and Deputy Doe 9's personnel record to be thoroughly prepared.

b. No Logical Inference

Counts 3 and 5 do not have sufficient logical inferences on the "access" element.

Count 3 relates to Deputy Doe 3 and Count 5, Deputy Doe 5. For each of these deputies, the documents relied on by the People were found in Allen Wang's files. Deputy Doe 3's document is Exhibit S, whereas Deputy Doe 5's document is Exhibit W. There are no corresponding emails indicating that the Defendant was concerned or was working on their writ process. In fact, both Deputy Doe 3 and Deputy Doe 5's writ process appear to have concluded prior to the Defendant taking on the role of Constitutional Policing Advisor in 2015. While Exhibit B, the tracker, shows each deputy on the spreadsheet, and, at least Deputy Doe 3's tracking has the same counsel listed as the writ, no evidence suggests that the Defendant went into PRMS on every entry on the tracker. The fact Wang had these in his files does not lead to a logical conclusion that the Defendant looked into PRMS for these deputies. As noted earlier, this is an instance where, although the deputies may be able to claim a breach of confidentiality, there is not a strong enough logical inference that the Defendant went into their PRMS in violation of section 502, subd. (c)(2).

2. Evidence of Knowing Use Without Permission

As noted above, counts 3 and 5 have failed at the first element. We now move on to the second element – knowingly using the data without permission.

The People presented four documents from the Sheriff's Manual of Policy and Procedures (MPP): 1) Exhibit BB entitled "Confidential Information"; 2) Exhibit CC entitled "Personnel Folders"; 3) Exhibit DD entitled "Prohibitions"; and 4) Exhibit EE entitled "Release of Information to Other Law Enforcement or Government Agencies." Taken together, the four MPP reinforces the rules set forth in section 832.7, subd. (a) on the confidential nature of a peace officer's personnel records and the process for the release of such records.

Exhibit EE states in pertinent part, "Authorized government agents and department personnel requesting information from official records shall submit a written request to the Records and Identification Bureau (RIB) or station desk officer … [o]nly properly identified representatives of the following agencies may be given access to requested information … authorized personnel of the District Attorney's Office …" (People's Exhibit EE.)

As previously discussed, the Defendant claims the writ documents are public records that do not belong to the Sheriff. The People's theory is not that the documents belonged to the Sheriff but that the name obtained from the personnel record, when linked to the sensitive confidential personnel record, is protected under section 832.7, sub. (a). Second, the Defendant posits she cannot be prosecuted for doing her job.

Defendant points to section 502, sub. (h)(1) which states, "[s]ubdivision (c) does not apply to punish any acts which are committed by a person within the scope of lawful employment. For purposes of this section, a person acts within the scope of employment when the person performs acts which are reasonably necessary to the performance of their work assignment." (Cal. Pen. Code § 502, sub. (h)(1).) In her closing summation, the Defendant asserts, "the evidence adduced at the preliminary hearing clearly established that Ms. Teran's official duties at the LADA's office required her to oversee and maintain the *Brady* and ORWITS databases. Section 502 (c) does not create liability for someone using data as part of their job responsibilities." (Defendant's Summation Brief, p. 7.)

The Legislative intent is not ambiguous. Section 502, subd. (a) states, "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 entity protected under the statute are 1) individuals, 2) businesses, and 3) governmental agencies to their lawfully created computer data and computer systems. (Cal. Pen. Code § 502, subd. (a).) The Los Angeles County District Attorney's Office did not create or maintain this data – the personnel records of peace officers that are kept in PRMS. The employer referenced under the statute's legislative intent here is the Sheriff, not the District Attorney. The People have met their burden of showing strong suspicion that the Defendant acted without the permission of the Sheriff when disclosing the names of Deputy Does 1, 2, 4, 7, 8, and 9 to DDA Revel without complying with the policy under People's Exhibit EE.

Next is the question of "use."

On this, the People showed the Defendant, on April 26, 2021, sent an email to DDA Revel and shared a folder as an attachment called "Writ Discipline Decision." (See People's Exhibit FF.) People's Exhibits GG, HH, and II are a list of the writ documents that were shared – which show that the writ documents corresponding to Deputy Does 1, 2, 4, 7, 8, and 9 were sent.

It is important to remember here that the data at issue is the name of the Deputy Does obtained from the personnel records, not the writ documents. The writ documents are the vehicle through which the names were disclosed. As stated previously, breach of confidentiality and violating section 502, subd. (c)(2) are not coequal to each other. As analyzed, *ante*, the People have – at least for purposes of the preliminary hearing – established a strong suspicion that the Defendant, went into the personnel records of Deputy Does 1, 2, 4, 7, 8, and 9 contemporaneous

to when she was working on their discipline matters. By bypassing the splash screen and accessing their names, the Defendant obtained the names of the Deputy Does 1, 2, 4, 7, 8, and 9 from the confidential personnel records. This also shows the names are linked to the sensitive and confidential personnel records. If the Defendant thereafter revealed their names obtained from PRMS by sending the writ documents which contains the name of the Deputy Doe, such sharing of the names constitutes knowing use of the data accessed through PRMS. Sharing the names of the Deputy Does 1, 2, 4, 7, 8, and 9 in the email attachment constitutes use of data.

D. Defendant's Other Contentions

The Defendant raises a few other contentions.

First, the Defendant argues section 502, sub. (c)(2) defines a single criminal act and that the "access" and "use" must be combined not separated by years as alleged by the People. (Defendant's Summation Brief, p. 11.) This interpretation appears inconsistent with the plain reading rule of statutory construction. By its wording, the statute requires two actions to fall under its ambit: 1) access, and 2) take, copy, or use. The statute does not restrict when the taking, copying or using must be accomplished. Say, a hacker obtains trade secrets of a successful business, waits three years for the statute of limitations to run from the date of access, then, uses the trade secret to the hacker's advantage. If Defendant's reading of the statute is accurate, such actions would fall outside the reach of section 502, sub. (c)(2). That cannot be so.

Defendant lastly argues the People's theory of using section 502, subd. (c)(2) under their theory is void for vagueness as applied.

"Unlike a facial challenge, where the defendant must show the statute is impermissibly vague in all of its application (citation omitted), the defendant making an as applied challenge must show that the statute is impermissibly vague as it was enforced against him in light of the facts and circumstances of his particular case. [Citation.] For an as applied challenge, we

evaluate the propriety of the application of the statute on a case-by-case basis. [Citation.]" (*People v. Agnelli* (2021) 86 Cal.App.5 th Supp. 1, 283 Cal.Rptr.3d 777, 780.)

" 'The starting point of our analysis is "the strong presumption that legislative enactments 'must be upheld unless their unconstitutionality clearly, positively, and unmistakably appears. [Citations.] A statute should be sufficiently certain so that a person may know what is prohibited thereby and what may be done without violating its provisions, but it cannot be held void for uncertainty if any reasonable and practical construction can be given to its language.' " [Citation.]' [Citation.]" (*People v. Hagedorn* (2005) 127 Cal.App.4th 734, 745)

"With respect to the determination whether a statute imparts fair warning, the United States Supreme Court has stated: '"There are three related manifestations of the fair warning requirement. First, the vagueness doctrine bars enforcement of 'a statute which either forbids or requires the doing of an act in terms so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application. [Citations.] Second, ..., the canon of strict construction of criminal statutes, or rule of lenity, ensures fair warning by so resolving ambiguity in a criminal statute as to apply it only to conduct clearly covered. [Citations.] Third, although clarity at the requisite level may be supplied by judicial gloss on an otherwise uncertain statute [citations], due process bars courts from applying a novel construction of a criminal statute to conduct that neither the statute nor any prior judicial decision has fairly disclosed to be within its scope [citations]. In each of these guises, the touchstone is whether the statute, either standing alone or as construed, made it reasonably clear at the relevant time that the defendant's conduct was criminal."" [Citation.]" (*Id.* at pp. 745-746.)

Due process requires a fair warning. The evidence introduced at the preliminary hearing through the testimony of Detective Bernstein established that, when a person accesses PRMS by logging into its system, such a person necessarily encounters a splash screen warning of possible prosecution under section 502. As noted, the prosecution is required to establish, either through

direct or circumstantial evidence, that the Defendant accessed PRMS. As applied to the facts of this case, for the reason stated above, the theory of the prosecution is not void for vagueness as applied, as a warning of possible prosecution had to be bypassed to prove knowing access.

This concludes the Court's statement of decision showing that the People have met their burden of reasonable suspicion as to Counts 1, 2, 4, 7, 8, and 9.

The statement of decision shall be filed and made part of the record of this case.

It is so ordered.

DATE 8/20/24

Judge Sam Ohta