Filed 6/1/21

CERTIFIED FOR PUBLICATION

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA

FIRST APPELLATE DISTRICT

DIVISION FOUR

THE PEOPLE, Plaintiff and Respondent, v. ERIC CURTIS LUND, Defendant and Appellant.	A157205 (Solano County Super. Ct. No. FCR310878)

A jury convicted Eric Lund of one count of possession of more than 600 images of child pornography, at least 10 of which involved a prepubescent minor or a minor under 12 years old, in violation of Penal Code section 311.11, subdivision (c)(1). The trial court sentenced Lund to five years in prison.

Lund contends the trial court committed four errors. First, he argues the trial court should have excluded some of the data produced by a computer program because the data was case-specific, testimonial hearsay under *People v. Sanchez* (2016) 63 Cal.4th 665 (*Sanchez*). Second, he argues the prosecution failed to establish that the computer program was reliable and generally accepted in the scientific community under *People v. Kelly* (1976) 17 Cal.3d 24 (*Kelly*) and *Sargon Enterprises, Inc. v. University of Southern California* (2012) 55 Cal.4th 747 (*Sargon*). Third, Lund urges that his conviction should be reversed because the prosecutor committed repeated, pervasive misconduct.

Finally, he argues that the trial court abused its discretion under Evidence Code section 352 in allowing the prosecution to play for the jury a number of child pornography videos. We reject each of these arguments and therefore affirm the judgment.

I. BACKGROUND

A. Peer-to-peer networks

Peer-to-peer networks allow sharing of files, including child pornography, over the internet. To access each different peer-to-peer network, users must download and install software that uses the programming protocol specific for that network. eDonkey is one example of a peer-to-peer network commonly used to share and download child pornography. eMule is a program people commonly use to get onto the eDonkey network.

When a user installs peer-to-peer networking software, the software randomly generates a globally unique identifier (GUID), which is used to specifically identify the instance of the software being used. The software also designates a five-digit port number, which is necessary for the software to communicate with the network. When a user sends out a search query, the request goes to one or more other "peer" computers in the network, which in turn propagate the request to other peers, and so on. This process exponentially increases the number of computers effectively receiving the search request. Each peer receiving the query will respond to the original user with a list of files matching the query that the peer has available for download. Despite the exponential spread of a search query, a user's query will not typically reach all other peers on the peer-to-peer

network and a user will not see every file from every computer on the network matching the query. When a computer connects to a peer-to-peer network, it will automatically start receiving queries from other users and returning a list of files that the computer has available. Peer-to-peer networks use hash values to identify each file being shared. A hash value is like a DNA signature for a digital file; it is statistically unique and never changes, so it provides a way to authenticate that two digital files are identical, even if the names are different.

B. CPS Software

In August 2014, Vacaville police detective Jeffrey Datzman was investigating child pornography cases over peer-to-peer networks. One of the tools Datzman used was privately-developed software called the Child Protection System (CPS). CPS is the web interface for viewing results from a suite of several software tools that each search for child pornography on a specific peer-to-peer network.[1] It is used around the world in 84 countries by over 10,000 users, all of whom are law enforcement personnel.

The CPS software suite automates the process of searching peer to peer networks. Previously, law enforcement officers would have to manually input keyword search terms to discover computers that were hosting suspected child pornography and then further investigate those GUIDs. By contrast, CPS sends

[1] Some of the CPS components include Peer Spectre, Nordic Mule, Gnew Watch, and GT Logger. For simplicity, we use CPS to refer both to the web interface and the underlying tools.

out search terms continuously. CPS also compares the files listed in response to the keyword searches against CPS's database of hash values, which contains the hash values of files that law enforcement officers somewhere in the world have previously tagged as being child pornography. If there is a match between the hash values for the files listed in response to the search and the hash values in the CPS database, CPS logs the details of the event in a CPS database for police officers to follow up on later. CPS logs the filenames and hash numbers of the suspected child pornography files being offered; the GUIDs, IP addresses, port number, and, in most cases, software used to offer the files; and the dates and times CPS detected the GUID with the files. Police officers obtain records from internet service providers to determine the physical location of the computer associated with the GUIDs, IP addresses, and port numbers logged by CPS.

A match between the hash number of a particular file being offered and a hash number in CPS's database suggests the file is likely child pornography. However, because child pornography laws can differ from one jurisdiction to another, CPS users are trained to always view a file personally in order to determine conclusively whether the file constitutes child pornography under applicable law. To assist with this, CPS also helps law enforcement users create their own separate, local databases of hash values called a media library. Where the CPS database contains only hash values and not the child pornography files, law enforcement users' media libraries contain both the hash values and the corresponding files. Users can use their media

libraries when they cannot download a file from the offering computer directly to view it. In such cases, users can compare the hash value of the file being offered to the hash value of a file in the media library and then use the media library file to confirm that the file is child pornography under applicable law.

C. Investigation of target GUID

When Datzman signed on to CPS in August 2014, he noticed that there was one user, identified by a specific GUID, who possessed several suspected child pornography files. Datzman downloaded a few files from the target GUID and confirmed that the files were in fact child pornography under California law. This GUID moved between different IP addresses but kept returning to a few addresses. This was unique, because GUIDs that moved from one IP address to another usually did not return to any of the IP addresses. After analyzing the target GUID's behavior, Datzman noticed that the GUID only showed activity overnight on Wednesday, Thursday, Friday, and Saturday nights. Because law enforcement officers often work overnight shifts four nights a week from Wednesday evening through Sunday morning, Datzman suspected that the target GUID user was a security guard, law enforcement officer, or someone else working such a shift.

Datzman obtained the physical addresses for the IP addresses the target GUID was using. Because the target GUID was active in the middle of the night when the businesses were closed, Datzman did not consider the owners of any of the IP addresses to be suspects. The most frequently recurring IP

address in Vacaville belonged to a business called the Yogurt Beach Shack, which was owned by two former law enforcement officers Datzman knew. Datzman confirmed that the Yogurt Beach Shack's wireless internet (wifi) router was "open," meaning it did not require a password, and could be accessed from outside the building. Datzman therefore conducted overnight surveillance at the Yogurt Beach Shack in early October 2014.

During the surveillance, Datzman connected to the Yogurt Beach Shack's router so that he could observe whether any devices connected to the router and see such devices' "mac ID," which is a unique specific identifier for a device. On one night, at around 1:00 a.m., Datzman saw a device connect to the router, and he recorded the mac ID. Datzman then drove around the outside of the building to see who was nearby that could be using the device. Datzman noticed a California Highway Patrol (CHP) vehicle parked near the business. Lund was the sole occupant of the vehicle, seated in the driver's seat and looking down and to his right at a lighted object. Datzman then contacted Sergeant Jason Johnson in the Vacaville Police Department. Johnson agreed to contact Lund using a ruse to determine his name. The ruse succeeded and Lund told Johnson his name. After Johnson spoke to Lund, Lund drove away, and Datzman noticed that the mac ID of the device that was using the Yogurt Beach Shack router dropped off at the same time. No other devices connected to the router that night. Datzman later checked CPS to see if the target GUID had been detected at the time that Lund was seen at the Yogurt Beach Shack. CPS had no record of it at that IP

address at that time, but it detected the GUID at a different router later that night.

Datzman contacted the CHP and learned from Lund's commanding officer that Lund was a sergeant assigned to the Fairfield CHP office, worked alone, and worked a schedule that matched the target GUID's pattern of activity. Lund lived in Chico, and stayed in a hotel in Vacaville during the days he was working.

Every CHP patrol vehicle has a computer with software installed that, when an officer logs into it, logs activity and also activates a global positioning system (GPS) location tracker. However, Lund had not logged into the software between June and October 2014, so there was no GPS data for him. Additionally, the dispatcher had recorded activity for him only three times during that span. This paucity of records was unusual and surprising. It was common knowledge among CHP officers that logging into the vehicle computer would transmit location data.

Datzman arranged with the commanding officer to put a GPS tracker on the two patrol cars assigned to CHP sergeants in the Fairfield office. The first night after the GPS trackers were installed, the GPS tracker showed that the car that Lund had been observed driving was stopped for over two hours at a location in Cordelia Park near a house with open wifi. CPS detected the target GUID with child pornography that night at that same location for about two hours.

D. Searches of devices in Lund's desk, car, and locker

Pursuant to search warrants, Vacaville police officers then searched Lund's desk at work and his personal car. Police found a flash drive in the center console of Lund's car. This flash drive did not contain child pornography. In the trunk of the car were Lund's CHP uniforms, his citation book, his old cell phone in a box, a USB wifi adaptor, and a tan backpack. Inside the backpack were two long range USB wifi adaptors with a panel antenna that could be used to pick up a wifi signal from greater distances, a laptop, two external hard drives, and three flash drives. One of the USB wifi adaptors had a mac ID identical to the one Datzman recorded from the router at the Yogurt Beach Shack.

The cell phone and one of the flash drives from the trunk of the car did not contain child pornography. This flash drive had been connected to a computer in Lund's home. The other two flash drives contained deleted child pornography videos and pictures that Datzman forensically recovered.

The external hard drives together contained over 10,000 files that Datzman suspected to be child pornography, based on their hash values' matches to the CPS database. Datzman reviewed a sample of 73 videos from the hard drives and confirmed that they were child pornography, with almost all of them containing at least one prepubescent minor. One of the hard drives also contained the same version of eMule that the target GUID used and the software necessary to use the panel antenna. Datzman concluded that one of the hard drives had

been used to store child pornography since 2012 because one of the folders on it indicated that eMule had been used with the hard drive since that date.

The laptop contained a copy of the eMule software with the same version number, GUID, and port number that CPS had detected. eMule had been used to download over 3,000 complete files whose names suggested they were child pornography. Like the flash drive from his desk and one of the hard drives, the laptop had the software necessary to use the panel wifi antenna. The laptop showed it had connected to the router at the Yogurt Beach Shack and had run eMule on the night Datzman and Johnson observed Lund there, but the program had crashed. The laptop also showed it had connected to the router where the IP address in Cordelia Park was located. The laptop had been used to access email and Facebook accounts, but the lack of activity in those accounts or information available about the named users indicated that the accounts did not belong to real people.

The laptop's last wifi connection was to the network at the Fairfield Inn in Vacaville an hour before Lund's arrest. This hotel was across the street from the hotel where Lund had a reservation and where his car was seen during the day of his arrest, before he came to the office. With a panel range antenna, the laptop could have accessed the Fairfield Inn's internet from Lund's room. The laptop's user viewed child pornography files throughout that day, and CPS detected the target GUID as being active throughout that day.

Lund's desk, which was known to other officers to be unlockable, contained Lund's active cell phone and three flash drives. All three flash drives showed they had been used with the computer on Lund's desk. None of the devices contained pornography, but one flash drive contained a copy of the eMule program and the software for the long range wifi adaptor found in the trunk of Lund's car.

About a week after Vacaville police searched Lund's desk and personal car, CHP officers searched Lund's locker at the Fairfield CHP building. They found hotel breakfast cards and a Diskgo flash drive with the first three digits of Lund's CHP badge number written on it. CHP Officer Ryan Duplissey took the Diskgo flash drive for analysis. In his report, Duplissey originally stated that the flash drive was found connected to Lund's work computer, but he later corrected his report to reflect that it was found in his locker. Datzman later acquired the drive and performed his own analysis. Both analyses showed the flash drive contained documents associated with Lund as well as 10 child pornography files that had been marked for deletion but could be forensically recovered. CHP officers also searched electronic devices found in Lund's home but did not find any child pornography on them.

E. Procedural history

After Lund was arrested and charged, pretrial litigation relating to the constitutionality of the searches stretched over the course of several years and involved two writ petitions to this court. A jury trial in the summer of 2018 resulted in a mistrial.

At the second trial in October 2018, the prosecution played for the jury brief portions of some of the child pornography files found on each device that Datzman had confirmed were child pornography.

Unlike the first trial, Lund testified in his own defense. He denied ever possessing or downloading child pornography. Lund said he was sitting in the Yogurt Beach Shack parking lot to eat and denied having a laptop in the car or connecting to the internet. He said the CHP computer in his vehicle, which was to the driver's right, would glow at night. He denied driving the patrol car that was recorded by GPS in Cordelia Park on the same night that CPS detected activity there and said he was in the office the whole night. On cross-examination, however, he admitted that he sent his wife a text that night saying he was going to go out and drive for fresh air. Lund also denied that the electronic devices found in his car, desk, or locker were his. He claimed other officers used his desk when he was not there. Lund testified that he never locked his locker because he had once forgotten the key at home in Chico and been unable to get his uniform, but he admitted on cross-examination this was not general knowledge. He said he kept hotel breakfast cards in his desk, not his locker, so someone at CHP must have moved them into the locker.

Lund explained he did not use the CHP computer in the patrol car because he thought it was unsafe. Lund said he instead used his radio to make requests through dispatch. He claimed the records of his radio activity were not obtained from

the correct office, and the proper records would have shown more activity. Lund admitted he had been suspended in 1996 for using a screensaver on his work computer that displayed adult pornography. Lund claimed that Datzman planted the evidence against him but had no theory for why.

In rebuttal, the prosecution called retired CHP Sergeant Steven Lott, who testified that officers used to tell him they could not reach Lund on the radio during his shifts. Lott also recalled that Lund would leave the office in the middle of the night complaining about the office being too hot or needing to stay awake, but it seemed like an excuse to leave the office.

The jury found Lund guilty and the trial court sentenced him to five years in prison.

II. DISCUSSION

A. Sanchez *error*

Lund first challenges the trial court's admission of the hash value information from the CPS database. He contends William Wiltse's and Officer Datzman's testimony about the CPS hash values corresponding to suspected child pornography files was inadmissible hearsay because the hash value database consists of out of court statements made by unidentified officers across the country and around the world.[2] He further argues the admission of this testimony violated his Sixth Amendment right to confront and cross-examine the witnesses against him.

[2] Wiltse oversees the development of the CPS software, and has himself written certain components of the software.

1. Relevant legal principles and standard of review

"[A] hearsay statement is one in which a person makes a factual assertion out of court and the proponent seeks to rely on the statement to prove that assertion is true. Hearsay is generally inadmissible unless it falls under an exception." (*Sanchez*, *supra*, 63 Cal.4th at p. 674.) "Documents like letters, reports, and memoranda are often hearsay because they are prepared by a person outside the courtroom and are usually offered to prove the truth of the information they contain." (*Id.* at pp. 674.) However, " '[o]nly people can make hearsay statements; machines cannot.' " (*Id.* at p. 690, fn. 16.)

The use of hearsay potentially conflicts with defendants' rights under the Sixth Amendment to the U.S. Constitution to confront witnesses against them. (*Sanchez*, *supra*, 63 Cal.4th at pp. 679–680.) As the California Supreme Court summarized, "In light of our hearsay rules and *Crawford* [*v. Washington* (2004) 541 U.S. 36 (*Crawford*)], a court addressing the admissibility of out-of-court statements must engage in a two-step analysis. The first step is a traditional hearsay inquiry: Is the statement one made out of court; is it offered to prove the truth of the facts it asserts; and does it fall under a hearsay exception? If a hearsay statement is being offered by the prosecution in a criminal case, and the *Crawford* limitations of unavailability, as well as cross-examination or forfeiture, are not satisfied, a second analytical step is required. Admission of such a statement violates the right to confrontation if the statement is testimonial hearsay, as the high court defines that term." (*Id.* at p. 680, italics omitted.)

Sanchez applied both steps of this inquiry to expert testimony. (*Sanchez*, *supra*, 63 Cal.4th at pp. 680, 687.) Experts had long been allowed to rely on hearsay when offering their opinions. (*Id.* at p. 676.) This rule arose because experts frequently acquire general knowledge in their field of expertise from third parties, but the rule was extended to apply to case-specific facts as well. (*Id.* at pp. 676, 678–679.) Case-specific facts are "those relating to the particular events and participants alleged to have been involved in the case being tried." (*Id.* at p. 676.) Courts had recognized the tension between experts' need to consider extrajudicial matters with defendants' interest in avoiding the substantive use of unreliable hearsay. (*Id.* at p. 679.) They had tried to balance these concerns by generally allowing experts to explain the bases for their opinions, even when those bases were general or case-specific hearsay, subject to an instruction that juries should only consider such hearsay as the basis for the expert's opinion and not for its truth. (*Ibid.*)

Sanchez concluded this was a mistake because a jury cannot avoid considering the truth of case-specific hearsay underlying an expert's testimony. (*Sanchez*, *supra*, 63 Cal.4th at pp. 679, 684.) *Sanchez* explained, "When an expert is not testifying in the form of a proper hypothetical question and no other evidence of the case-specific facts presented has or will be admitted, there is no denying that such facts are being considered by the expert, and offered to the jury, as true." (*Id.* at p. 684.) The court therefore adopted "the following rule: When any expert relates to the jury case-specific out-of-court

statements, and treats the content of those statements as true and accurate to support the expert's opinion, the statements are hearsay. It cannot logically be maintained that the statements are not being admitted for their truth. If the case is one in which a prosecution expert seeks to relate *testimonial* hearsay, there is a confrontation clause violation unless (1) there is a showing of unavailability and (2) the defendant had a prior opportunity for cross-examination, or forfeited that right by wrongdoing." (*Id.* at p. 686, fn. omitted.) *Sanchez* noted, however, that experts can still "rely on information within their personal knowledge, and they can give an opinion based on a hypothetical including case-specific facts that are properly proven. They may also rely on nontestimonial hearsay properly admitted under a statutory hearsay exception." (*Id.* at p. 685.)

As to the second step of the hearsay inquiry, *Sanchez* reviewed several Supreme Court decisions dealing with statements made to police officers and summarized, "Testimonial statements are those made primarily to memorialize facts relating to past criminal activity, which could be used like trial testimony. Nontestimonial statements are those whose primary purpose is to deal with an ongoing emergency or some other purpose unrelated to preserving facts for later use at trial." (*Sanchez*, *supra*, 63 Cal.4th at p. 689.)

Sanchez did not address the standard of review for determining whether a statement is case-specific, testimonial hearsay. As the first step of the analysis is a "traditional hearsay inquiry" into whether a statement was made out of court and is

offered for its truth, we apply the abuse of discretion standard at this step. (*Sanchez*, *supra*, 63 Cal.4th at p. 680.) "A trial court's decision to admit or exclude evidence is reviewed for abuse of discretion, and it will not be disturbed unless there is a showing that the trial court acted in an arbitrary, capricious, or absurd manner resulting in a miscarriage of justice." (*People v. Wall* (2017) 3 Cal.5th 1048, 1069.) By contrast, *Sanchez*'s second step, concerning whether a statement is testimonial, implicates the constitutional right of confrontation, so we independently review that issue. (*People v. Nelson* (2010) 190 Cal.App.4th 1453, 1466.)

2. Analysis

Lund contends testimony from both Wiltse and Datzman violated *Sanchez* because both witnesses relied on CPS's database of hash values corresponding to previously identified child pornography. As to Wiltse, Lund asserts that Wiltse testified that CPS uses its hash value database to search peer-to-peer networks and that officers can determine whether a file offered by a suspect is child pornography, even if they cannot download the file, by comparing the file's hash value to CPS's hash value database. Lund also contends that both Wiltse and Datzman testified that CPS showed the target GUID downloaded a file that CPS had tagged as child pornography. As to Datzman, Lund asserts that Datzman opined that the hash value of a file is very important to determining whether the file is child pornography. Lund also cites Datzman's testimony that he used a computer program to compare the hash values of files on the hard drives found in Lund's trunk to the CPS hash value

database and Datzman's opinion that the hard drive had been using eMule to obtain child pornography as early as 2012.

Lund argues this testimony violates *Sanchez* because it is case-specific, testimonial hearsay. He contends it is case-specific hearsay because the entirety of the case against him was based on the CPS data and CPS cannot work without the assumption that whoever put a hash value in the CPS database correctly tagged it as child pornography. He argues the CPS hash value data is testimonial because it represents the fruits of previous law enforcement investigations.

We conclude the trial court did not abuse its discretion in determining the CPS hash values were not hearsay in this case because they were not admitted for their truth, so we do not reach the question of whether the hash values are testimonial.[3]

Preliminarily, Lund's *Sanchez* arguments regarding the CPS hash values rest on a misinterpretation of the record, stemming from the fact that the CPS software relies on hash values in two separate databases. First, CPS maintains a database of hash values on its own servers, without associated files. It uses this database as part of its searches of peer-to-peer networks. CPS uses keywords to search the peer-to-peer networks, then matches the hash values of the files that are listed in response to those keyword searches against the CPS

---

[3] While we apply the abuse of discretion standard in this case, as explained above, we would reach the same conclusion even if we were to independently review the trial court's conclusion that the CPS hash values are not hearsay.

database of hash values of suspected child pornography. In cases where the hash values match, the software logs the file being offered on the peer to peer network as suspected child pornography and saves the record for law enforcement officials to review later.

Second, CPS assists law enforcement officers with maintaining a media library, which is a local database of child pornography files and associated hash values. Police officers use this media library, not the CPS hash value database, to determine whether a file that they cannot download from a suspect is in fact child pornography. The police officer does so by matching the hash value of the suspect's file to the hash value of a file in the library. Using the copy of the file in the media library, the officer can opine conclusively that the file is child pornography.

Wiltse and Datzman explained carefully and repeatedly that the only way to determine whether a file is child pornography is for an officer to personally view a file or have personally viewed an identical copy of the file (meaning a matching hash value) in the past. This is because the police officer who input a hash value in the CPS database could have erred, and because the legal definitions of child pornography differ between jurisdictions. Wiltse testified consistently that the hash value database exists to create criminal leads about suspected but unconfirmed child pornography, not to provide definitive proof that any file is child pornography. Moreover, Datzman's conclusion that the hard drive had been used to store

downloaded child pornography since 2012 was not based on the CPS hash values, but rather on the fact that there were folders indicating that eMule had been used with the hard drive since then.

This proper understanding of the record regarding CPS demonstrates why Lund's *Sanchez* argument fails at the first step. " 'Out-of-court statements that are not offered for their truth are not hearsay under California law [citations], nor do they run afoul of the confrontation clause.' " (*People v. Bell* (2019) 7 Cal.5th 70, 100.) Neither Wiltse nor Datzman relied on the CPS hash values for their truth to opine that any file was child pornography. The prosecution used Wiltse's and Datzman's testimony about the hash values only to explain Datzman's course of conduct in investigating the GUID and Lund. Lund's defense that Datzman or someone else planted the evidence in his car, desk, and locker made it fair for the prosecution to show that Datzman followed reasonable leads. This is an example of the principle that " ' " '[e]vidence of a declarant's statement that is offered to prove that the statement imparted certain information to the hearer and that the hearer, believing such information to be true, acted in conformity with that belief . . . is not hearsay, since it is the hearer's reaction to the statement that is the relevant fact sought to be proved, not the truth of the matter asserted in the statement.' " ' " (*Ibid.*) Even if every entry in the CPS hash value database were wrong, such hypothetical errors would not undermine the prosecution's proof of the elements of the charge against Lund. The prosecution proved the

files found on devices associated with Lund were pornography either by showing them to the jury or by having Datzman testify that he personally viewed them and verified that they met the legal description.[4]

Even if Lund were correct that the CPS hash value data constituted hearsay that was also testimonial, its admission was harmless beyond a reasonable doubt. (See *Sanchez*, *supra*, 63 Cal.4th at p. 698 [applying federal standard of harmlessness beyond a reasonable doubt to violation of Confrontation Clause through admission of testimonial hearsay].) At its core, the prosecution proved its case by establishing that the police found child pornography on electronic devices found in Lund's locker and in the trunk of his car. These devices were found in locations within his control, particularly his car. This evidence is circumstantial but strongly persuasive, especially because Lund

---

[4] The facts of this case are therefore distinguishable from cases like *U.S. v. Juhic* (8th Cir. 2020) 954 F.3d 1084, 1088–1089, and *U.S. v. Bates* (11th Cir. 2016) 665 Fed.Appx. 810, 814–815, which held that CPS reports were inadmissible testimonial hearsay. In those cases, it appears the prosecution used the reports' notation that certain files had been previously identified as child pornography as evidence that files were indeed child pornography. (*Juhic*, at p. 1089 [CPS reports were "out-of-court statements offered for the truth of the matter asserted: that the videos and images were child pornography"]; *Bates*, at p. 815 ["The record shows that the government used the reports to demonstrate the steps of [the officer's] investigation and to prove that the files [the defendant] downloaded were child pornography"].) There is no indication in these decisions that any witnesses identified any files as child pornography after viewing them, like Datzman did here.

does not explain how someone would have gained access to his car.

Lund notes that the cell phone and the flash drive found in his trunk, which had been connected to a computer in his home, contained no child pornography. He therefore asserts that none of the digital devices containing child pornography could be linked to him. This argument ignores the critical fact of the devices found in the trunk of his car, as well as the flash drive found in his locker. That flash drive, which contained deleted child pornography, could be tied to Lund both by its location and by the presence of Lund's files on it. It was not common knowledge that Lund's locker was unlocked. Lund contended the devices were planted, but he offered the jury no reason why Datzman or any of the officers who performed the searches of his car, desk, and locker would have wanted to frame him or had the opportunity to do so.

Lund also takes the position that the theory that he used eMule to download child pornography was essential to the prosecution's case. He observes that the CPS evidence helped refute Lund's defense that the electronic devices were planted by showing Lund was at the same locations as the devices containing the pornography. While the CPS evidence was not legally essential, it was certainly helpful for rebutting Lund's defense. But the CPS data that rebutted the defense was the date, time, and IP address information, since these types of data helped establish the connections with Lund's movements. The GUID, eMule version number, and port also helped connect Lund

to the laptop found in his trunk. The CPS hash values were not helpful to this rebuttal. For example, if CPS had logged the target GUID as offering some other type of file, like copyrighted movies or music, the CPS location-related and laptop-related data would have been just as powerful for the prosecution's effort to undermine Lund's defense.

Lund does not argue CPS's date, time, IP address, GUID, version number, or port data are hearsay, nor could he, because they were all generated automatically by the CPS software. (*Sanchez*, *supra*, 63 Cal.4th at p. 690, fn. 16 [" 'Only people can make hearsay statements; machines cannot' "].) Lund instead appears to assume that if the CPS hash values were hearsay, the rest of the CPS data would have been excluded. This assumption is unfounded, as the hash values could easily have been omitted from the relevant exhibits and testimony. Lund also maintains the CPS hash value data helped establish that Datzman conducted a thorough investigation, in response to Lund's attempts to show the investigation was flawed. This is true, but Lund's attacks on the investigation's minor flaws were not so strong that the CPS hash value evidence was necessary to refute them, and thus the admission of that evidence—even if erroneous—did not cause prejudice.

B. **Kelly *and* Sargon *error***

In his second argument, Lund argues the trial court should have granted his motion in limine to exclude evidence of CPS entirely because the prosecution failed to establish that CPS satisfied the standard for admission of new scientific evidence

under *Kelly*, *supra*, 17 Cal.3d 24, and because the trial court failed to perform its gatekeeping function under *Sargon*, *supra*, 55 Cal.4th 747. He argues the admission of CPS evidence rendered his trial fundamentally unfair in violation of the 14th Amendment and was not harmless under the federal or state standards.

1. Relevant legal principles and standard of review

a. Kelly

"*Kelly* was the genesis of a rule, previously called the '*Kelly*/*Frye* rule,' [5] that governs the admissibility of evidence derived from new scientific techniques. 'Under *Kelly*, the proponent of evidence derived from a new scientific technique must establish that (1) the reliability of the new technique has gained general acceptance in the relevant scientific community, (2) the expert testifying to that effect is qualified to give an opinion on the subject, and (3) the correct scientific procedures were used.' " (*People v. Jones* (2013) 57 Cal.4th 899, 936.) "The purpose of these threshold requirements—commonly referred to as the *Kelly* test—is to protect against the risk of credulous juries attributing to evidence cloaked in scientific terminology an aura of infallibility." (*People v. Peterson* (2020) 10 Cal.5th 409, 444 (*Peterson*).)

"Not every subject of expert testimony needs to satisfy the *Kelly* test. Courts determining whether *Kelly* applies must

---

[5] "See *Frye v. U.S.* (D.C.Cir.1923) 293 F. 1013, 1014, superseded by statute as explained in *Daubert v. Merrell Dow Pharmaceuticals, Inc.* (1993) 509 U.S. 579 [(Daubert)]."

consider, first, whether the technique at issue is novel, because *Kelly* ' "only applies to that limited class of expert testimony which is based, in whole or part, on a technique, process, or theory which is new to science and, even more so, the law." ' [Citation.] Second, courts should consider whether the technique is one whose reliability would be difficult for laypersons to evaluate. A '*Kelly* hearing may be warranted when "the unproven technique or procedure appears in both name and description to provide some definitive truth which the expert need only accurately recognize and relay to the jury." ' [Citation.] Conversely, no *Kelly* hearing is needed when '[j]urors are capable of understanding and evaluating' the reliability of expert testimony based in whole or in part on the novel technique." (*Peterson*, *supra*, 10 Cal.5th at p. 444.)

"Appellate courts review de novo the determination that a technique is subject to *Kelly*." (*People v. Jackson* (2016) 1 Cal.5th 269, 316.)

b. Sargon

Regardless of whether expert evidence relates to a new scientific technique under *Kelly*, a trial court must ensure that expert testimony has a sufficient basis to merit the jury's consideration. (*Sargon*, *supra*, 55 Cal.4th at p. 770.) "[U]nder Evidence Code sections 801, subdivision (b), and 802, the trial court acts as a gatekeeper to exclude expert opinion testimony that is (1) based on matter of a type on which an expert may not reasonably rely, (2) based on reasons unsupported by the material on which the expert relies, or (3) speculative." (*Id.* at

pp. 771–772.) "The trial court's preliminary determination whether the expert opinion is founded on sound logic is not a decision on its persuasiveness. The court must not weigh an opinion's probative value or substitute its own opinion for the expert's opinion. Rather, the court must simply determine whether the matter relied on can provide a reasonable basis for the opinion or whether that opinion is based on a leap of logic or conjecture. The court does not resolve scientific controversies. Rather, it conducts a 'circumscribed inquiry' to 'determine whether, as a matter of logic, the studies and other information cited by experts adequately support the conclusion that the expert's general theory or technique is valid.' [Citation.] The goal of trial court gatekeeping is simply to exclude 'clearly invalid and unreliable' expert opinion. [Citation.] In short, the gatekeeper's role 'is to make certain that an expert, whether basing testimony upon professional studies or personal experience, employs in the courtroom the same level of intellectual rigor that characterizes the practice of an expert in the relevant field.' " (*Id.* at p. 772.)

"Except to the extent the trial court bases its ruling on a conclusion of law (which we review de novo), we review its ruling excluding or admitting expert testimony for abuse of discretion." (*Sargon*, *supra*, 55 Cal.4th at p. 773.)

2. Analysis

a. Kelly

Lund argues the trial court should have excluded all evidence regarding CPS under *Kelly* because CPS is an unproven,

largely untested, and inherently unreliable computer program. He contends it had the appearance of reliability but there was no evidence that CPS was widely accepted or that CPS followed the correct procedures.

Lund's argument bypasses the threshold *Kelly* question of whether the testimony about CPS is part of " ' "that limited class of expert testimony which is based, in whole or part, on a technique, process, or theory which is new to science and, even more so, the law," ' " whether it " 'appears in both name and description to provide some definitive truth which the expert need only accurately recognize and relay to the jury,' " and whether jurors " 'are capable of understanding and evaluating' the reliability of expert testimony based in whole or in part" on CPS. (*Peterson*, *supra*, 10 Cal.5th at p. 444.) Instead, he simply assumes both that CPS itself is a scientific process or technique, rather than a program using such a technique, and that it was novel. These assumptions are misplaced. CPS is not a technique or process; it is a program that deploys a technique or executes a process. (Cf. *People v. Nolan* (2002) 95 Cal.App.4th 1210, 1215 ["a *Kelly*/*Frye* hearing is not required for new devices; it applies to new methodologies"]; *People v. Lazarus* (2015) 238 Cal.App.4th 734, 782–786 [distinguishing between new DNA test kit and the existing technique it used].) And the technique or process that CPS uses is not novel, nor is it so persuasive that it threatens to beguile a jury with misleading scientific certainty.

Before CPS, a police investigator investigating peer-to-peer networks had to manually enter search terms in a software

program, record the results, and follow up on leads by obtaining records from internet service providers to connect IP addresses to physical locations. The only novelty in CPS lies in its approach of automating the pre-existing search process. Instead of officers needing to perform manual searches during working hours and noting the pertinent information regarding any leads, CPS runs searches around the clock and has the computer log the relevant details regarding leads. (*U.S. v. Thomas* (2d Cir. 2015) 788 F.3d 345, 348 [describing CPS's operation].) CPS's process or technique, then, is simply to perform the same searches that law enforcement officers used to do, but in larger volume and at all times of the day, and record the results for later perusal.

CPS's ability to generate a larger volume of search results over a longer period of time undoubtedly makes it a useful, time-saving device. It also unlocks the possibility of using the search results for different purposes, such as the prosecution's approach here of using CPS results to map the behavior and location of the target GUID over time. But CPS's results themselves do not purport to offer any more scientific or technical certainty regarding the data they contain than the manual searches CPS replaced. Computers are now commonplace, so the general public can be expected to be generally familiar with the notions that software can repeatedly perform simple tasks that previously would have taken extensive human labor to complete in the same quantity and that the resulting quantity of data can be analyzed and used in different ways that were not possible before. We do not see how CPS's addition of automation to the routine police

work of finding and recording evidence is so mysterious or seemingly authoritative that it would be difficult for laypersons to understand or evaluate it. As a federal district court remarked when considering the admissibility of evidence from software like CPS, "Computer programming is not a scientific theory or technique, it is not new or novel, and it does not implicate the [c]ourt's responsibility to keep 'junk science' out of the courtroom. Any doubts about whether [the software] operates in the manner that [its creator] represents go to the weight, and not the admissibility, of his testimony." (*United States v. Blouin* (W.D. Wash., Aug. 15, 2017, No. CR16-307 TSZ) 2017 WL 3485736, *7.)[6]

The prosecution's use of CPS can be analogized to the computerized fingerprint matching program challenged in *People v. Farnam* (2002) 28 Cal.4th 107. In that case, the police had used a computerized database for fingerprint matching to produce a list of candidates, including the defendant, whose fingerprints resembled those at the crime scene. (*Id.* at p. 159.) Fingerprint analysts then compared the defendant's fingerprint to a fingerprint found at the crime scene and concluded they matched. (*Ibid.*) The California Supreme Court held that the evidence regarding the computerized fingerprint matching program did not implicate *Kelly*. (*Id.* at p. 160.) The expert who

---

[6] Though the federal *Daubert* standard for admission of scientific evidence differs somewhat from the *Kelly* standard, appellate decisions affirming the admission of scientific evidence under that standard are relevant to the *Kelly* analysis. (*People v. Venegas* (1998) 18 Cal.4th 47, 88 [relying in part on state court decisions using the *Daubert* standard]; *People v. Buell* (2017) 16 Cal.App.5th 682, 690–691 [same].)

relied on the database never claimed that the database positively identified the defendant's print. (*Ibid.*) The jurors could determine the reliability of the database by comparing the defendant's fingerprint to that found at the crime scene. (*Ibid.*) And no opinion regarding the fingerprint identification was based on the computer results. (*Ibid.*) The mere use of the computer system to narrow the range of potential candidates was insignificant because the prosecution relied on the long-established method of expert fingerprint comparison to show the defendant's prints matched. (*Ibid.*)

People v. Johnson (2006) 139 Cal.App.4th 1135 followed *People v. Farnam* in the context of a DNA database. There, a lab technician obtained a DNA profile obtained from analysis of a sexual assault examination kit taken from the victim. (*Johnson,* at p. 1143.) The technician submitted the sample to a computerized DNA database and found a match to the defendant. (*Ibid.*) A blood sample was then taken from the defendant, and the technician matched the DNA profiles of the rape kit sample and the defendant's sample. (*Ibid.*) The court affirmed the admission of this DNA evidence, in part because the DNA analysis techniques at issue had been generally accepted for some time. (*Id.* at p. 1149.) But the court further rejected the defendant's argument that the expert erred in calculating the probability of a match between a random person and the rape kit DNA profile. (*Ibid.*) The court stated, "the use of database searches as a means of identifying potential suspects is not new or novel," because DNA databases and data bank statutes have

been enacted in all 50 states and by the federal government. (*Ibid.*) The court made clear that its "core point" was that "the database search merely provides law enforcement with an investigative tool, not evidence of guilt." (*Id.* at p. 1150.) In the court's view, "the means by which a particular person comes to be suspected of a crime—the reason law enforcement's investigation focuses on him—is irrelevant to the issue to be decided at trial, i.e., that person's guilt or innocence, except insofar as it provides *independent* evidence of guilt or innocence." (*Ibid.*)

Like the fingerprint database in *People v. Farnam*, *supra*, 28 Cal.4th at page 159 or the DNA database in *People v. Johnson*, *supra*, 139 Cal.App.4th at page 1149, CPS automated the process of searching for computers suspected of containing child pornography. But as in those cases, a police officer, Datzman—not CPS—made the ultimate conclusion that the files on the devices linked to Lund were child pornography. The prosecution's use of CPS went slightly beyond the fingerprint or DNA databases in those cases, since the prosecution relied on CPS to match the target GUID's patterns and locations to Lund's schedule and movements. In this regard, the CPS information could be said to provide, as the court put it in *Johnson*, at page 1150, evidence of guilt independent of the child pornography found on the devices. Nonetheless, we do not view this fact as significant because, as in *People v. Farnam*, the reliability of this information was readily apparent to the jury.

The CPS data had no aura of authority on its own because CPS had no records mentioning Lund specifically or matching to

an address that could be tied to him. The CPS evidence was only persuasive to the extent that the target GUID's behavior and locations matched Lund's schedule and movements, and the jury was well-equipped to evaluate whether the two matched. The prosecution's evidence on that point was also strong. At precisely the time that Datzman observed a device access the router at the Yogurt Beach Shack and then drop off, Datzman and Johnson observed Lund in his police car outside the business and then drive away. The long range antenna found in Lund's trunk matched the mac ID Datzman observed access the router. The antenna was used with the laptop found in the trunk. The laptop had accessed the router at the Yogurt Beach Shack at the same time Lund was there. The laptop also had a copy of eMule with the same GUID and port number that CPS detected. The laptop accessed the router near Cordelia Park, at the same time that CPS detected the GUID there and the police car Lund was driving was located by GPS there. CPS detected the GUID using the Fairfield Inn internet at the same time Lund's car was observed at the hotel nearby, where he also had a reservation. The only point on which CPS did not match Lund's movements was that CPS did not detect the GUID at the Yogurt Beach Shack when Lund was there. But Datzman's later analysis of the laptop suggested it was because the eMule program crashed when Lund was trying to use it there.

The jury could evaluate the credibility of the individual witnesses' testimony that the prosecution used to establish Lund's movements, and then determine for itself whether that

testimony matched the data from CPS. CPS did not have any particular heightened power to dazzle the jury, so there was no need to hold a *Kelly* hearing to evaluate it.

b. Sargon

Even though *Kelly* did not apply to the CPS evidence, the trial court was still obligated under *Sargon* to exclude the CPS testimony if it was "(1) based on matter of a type on which an expert may not reasonably rely, (2) based on reasons unsupported by the material on which the expert relies, or (3) speculative." (*Sargon*, *supra*, 55 Cal.4th at pp. 771–772.) Lund contends Wiltse's and Datzman's expert testimony based on CPS failed under *Sargon* because there was insufficient evidence to show that CPS reliably worked. We disagree.

The trial court did not abuse its discretion in finding Wiltse provided sufficient information to demonstrate CPS was reliable enough to be presented to the jury. Wiltse opined directly, as an expert, that the software is reliable and widely used in 84 countries by over 10,000 licensed users. Wiltse wrote the code for many of the tools in the CPS, and he oversaw the development of others as a supervisor. Wiltse had never had a complaint from users that CPS's leads were unsubstantiated. CPS itself had never been hacked or corrupted by an external source. Wiltse tested the program extensively in a closed environment to ensure its accuracy before using it on the wider internet. Wiltse explained this initial testing was sufficient because there was no way to test it outside the closed environment and until the peer-to-peer network protocol changed, there was no need to change

the CPS software. Wiltse had testified before as an expert in Oregon, Illinois, Utah, New Mexico, Vermont, and Florida, and had twice participated in court-ordered testing of the program for federal courts in California. Wiltse was not aware of any convictions ever being reversed as a result of him being allowed to testify about CPS.

Lund offers several theories as to how Wiltse failed to prove CPS's reliability, such as the contentions that Wiltse improperly assumed that the peer-to-peer protocols did not change, failed to show the software remained reliable after its release, relied on the absence of anecdotal reports of error to conclude the software was reliable, and did not subject the software to third-party testing. These arguments are speculative. Lund cross-examined Wiltse at the pre-trial hearing and at trial about any flaws in CPS or need for third party testing, but he did not succeed in casting any doubt on its operations. Nor has Lund presented in this court any specific reasons to discount Wiltse's testimony. To the contrary, the trial court could have reasonably concluded that the pre-release testing and track record of success demonstrated that CPS was sufficiently reliable to provide the basis for Wiltse's and Datzman's testimony.

Lund contends Wiltse should have provided more detail about how CPS worked, such as its source code and how it determined what items to search for and where to search for them. He also argues there was no evidence about how CPS stored information, how it chose what information to store, and how CPS took information from the peer-to-peer network and

saved it within the CPS program. But Wiltse explained that CPS searches using terms commonly associated with child pornography files, and its different component programs searched different peer-to-peer networks that commonly offered child pornography. He talked about how CPS populated its database with information other computers provided in response to queries of the peer-to-peer networks or, in the case of hash values, by CPS users worldwide. He also detailed how the CPS component used here, Nordic Mule, logs its own dates and times that files are being offered and makes direct connections to computers hosting suspected child pornography to verify those IP addresses, so that those fields in its database are absolutely accurate. Lund does not cite authority for or explain how technical detail about the source code or algorithms was required (or even helpful) to establish CPS's reliability.

Finally, we note that many courts have concluded CPS is sufficiently reliable to provide probable cause for a search under the Fourth Amendment. (E.g., *U.S. v. Thomas*, *supra*, 788 F.3d at p. 353 ["we discern no error—much less, clear error—in the District Court's finding that CPS was a reliable tool that could serve as the basis of a search warrant affidavit"]; *U.S.A. v. McKinion* (C.D. Cal., July 21, 2017, No. 2:14-CR-00124-CAS-1) 2017 WL 3137574, at *4, fn. 7; *U.S. v. Collins* (S.D. Iowa 2009) 753 F.Supp.2d 804, 809 [Peer Spectre, one of the CPS component tools, "is routinely and widely used by law enforcement officers to conduct [peer-to-peer] investigations, with wide-ranging acceptance for reliability," notwithstanding the defendant's

expert's claims to the contrary]; *U.S. v. Naylor* (S.D. W.Va. 2015) 99 F.Supp.3d 638, 643 [finding, based in part on police officer's experience of 100% reliability of CPS in 50 cases, that "CPS software appears to be a reliable investigative tool for law enforcement"]; *People v. Worrell* (N.Y. Sup. Ct. 2018) 71 N.Y.S.3d 839, 854, affd. (N.Y. App. Div. 2019) 170 A.D.3d 1048 [noting how numerous state and federal courts had rejected Fourth Amendment challenges to the use of CPS in part because courts "have repeatedly found CPS to be . . . a reliable investigative tool"].) Lund has cited and our research has discovered no case that has determined in any context that evidence from CPS or programs like it is unsupported or unreliable. The apparently

uniform acceptance and reliance on CPS evidence supports the trial court's decision to admit the CPS evidence here.[7]

C. Prosecutorial misconduct

Next, Lund argues the prosecutor engaged in repeated, pervasive misconduct that violated state law and rendered his trial fundamentally unfair, denying him his federal right to due process. Lund bases these contentions on four areas of alleged misconduct by the prosecutor: asking objectionable questions, engaging in repeated argumentative questioning, asking Lund to comment on the testimony of other witnesses, and testifying as a witness. He further asserts the pervasive nature of the

---

[7] Our holdings that the prosecution's CPS evidence did not need to undergo *Kelly* review and was admissible under *Sargon* should not be taken to preclude inquiry, through cross-examination or discovery, into the possible fallibility of the software. Lund was still entitled to attack the weight of that evidence, which he might have done by, for example, examining the source code and pointing out any flaws in its operation. (See, e.g., *U.S. v. Budziak* (9th Cir. 2012) 697 F.3d 1105, 1111–1113 [district court abused its discretion in denying discovery into software like CPS]; *U.S. v. Hartman* (C.D. Cal., Nov. 24, 2015, No. SACR 15-00063-JLS) 2015 U.S. Dist. Lexis 197382 at *30–*41 [allowing discovery into software used to investigate peer-to-peer networks, including two components of CPS].) Lund initially sought the CPS source code from the prosecution in discovery, and the prosecution did not dispute that such evidence was relevant. The trial court denied his request because it concluded CPS's creators were not part of the prosecution team for the purposes of criminal discovery, but it did so without prejudice to Lund seeking such evidence via subpoena. There is no indication in the record that Lund sought the source code via subpoena.

misconduct was prejudicial under both state and federal standards for reversal. We are not persuaded.

1. Relevant legal principles

" ' "A prosecutor who uses deceptive or reprehensible methods to persuade the jury commits misconduct, and such actions require reversal under the federal Constitution when they infect the trial with such ' "unfairness as to make the resulting conviction a denial of due process." ' " ' [Citation.] ' "Under state law, a prosecutor who uses such methods commits misconduct even when those actions do not result in a fundamentally unfair trial." ' [Citation.] . . . Prosecutorial misconduct can result in reversal under state law if there was a 'reasonable likelihood of a more favorable verdict in the absence of the challenged conduct' and under federal law if the misconduct was not 'harmless beyond a reasonable doubt.' " (*People v. Rivera* (2019) 7 Cal.5th 306, 333–334.) A showing of bad faith is not required to establish prosecutorial misconduct; "the term prosecutorial 'misconduct' is somewhat of a misnomer to the extent that it suggests a prosecutor must act with a culpable state of mind. A more apt description of the transgression is prosecutorial error." (*People v. Hill* (1998) 17 Cal.4th 800, 823, fn. 1.)

" 'As a general rule a defendant may not complain on appeal of prosecutorial misconduct unless in a timely fashion—and on the same ground—the defendant made an assignment of misconduct and requested that the jury be admonished to disregard the impropriety.' " (*People v. Prieto* (2003) 30 Cal.4th 226, 259.) " '[O]nly if an admonition would not have cured the

harm is the claim of misconduct preserved for review.' " (*People v. Friend* (2009) 47 Cal.4th 1, 29.)

2. Analysis

a. Repeated objectionable questions

We begin with Lund's argument that the prosecutor committed misconduct by repeatedly asking him objectionable questions during cross-examination. Lund contends that it is misconduct for a prosecutor to purposefully try to elicit inadmissible testimony, especially after defense counsel has objected or a trial court has already ruled. He claims the prosecutor violated this principle by (a) posing five questions that had previously been asked and answered, (b) asking several questions that infringed on the attorney-client privilege, and (c) asking him to discuss other evidence introduced at trial that was outside his personal knowledge, even though the trial court repeatedly sustained his objections to all of the questions.

Lund did not raise in the trial court his argument that the pattern of the prosecutor's behavior constituted misconduct. However, he did raise the issue of misconduct with respect to the questions that he contends intruded on the attorney-client privilege, and the trial court sua sponte admonished the prosecutor with regard to some of her questions asking Lund about other evidence at trial. We therefore conclude the issue has been sufficiently preserved for review on appeal.

The prosecutor's questions do not rise to the level of misconduct. Lund cites cases holding that a prosecutor may commit misconduct by intentionally seeking to admit

inadmissible evidence. (*People v. Smithey* (1999) 20 Cal.4th 936, 960; *People v. Bell* (1989) 49 Cal. 3d 502, 532; *People v. Johnson* (1978) 77 Cal.App.3d 866, 873–874.) But those cases involved situations in which prosecutors tried to introduce evidence that was inadmissible in its entirety, particularly when the trial court had already so ruled. The principle illustrated by those decisions is not on point here, where the prosecutor asked Lund the same questions he had already answered or asked him questions designed to contrast his testimony with evidence that had already been admitted. To be sure, a prosecutor may engage in misconduct by repeatedly asking these types of questions, but such repetition would have to be far more extensive than the few questions Lund highlights. (*People v. Armstrong* (2019) 6 Cal.5th 735, 795–796 [hostile, repetitive, and argumentative cross-examination of capital murder defendant was not misconduct].)

Lund's argument based on the attorney-client privilege is unpersuasive, but for a different reason. The prosecutor asked Lund whether a computer expert gave Lund any reason to doubt Datzman's testimony, whether Lund called that expert at trial, whether Lund would have called the expert if the expert could dispute Datzman's actions, and whether Lund hired the expert but decided not to call him. Lund objected to these questions on bases other than attorney-client privilege, and the trial court sustained the objections though not necessarily for the reasons Lund asserted. Lund later argued outside the jury's presence that the questions were misconduct because they intruded on the attorney-client privilege. The trial court indicated it had

sustained some of Lund's objections because of the privilege and said that if the issue recurred it would admonish the jury to disregard questions to which the court sustained an objection. But the prosecutor said she was done with that area of questioning, so the issue did not recur.

Reasonable minds might differ, but the trial court did not abuse its discretion in sustaining objections to the prosecutor's questions, since they perhaps could have called for discussions of trial strategy. But we find no merit in Lund's contention that the questions constituted misconduct by allowing the jury to infer that he did not call the expert because the expert's testimony would not have helped his defense. "[P]rosecutorial comment upon a defendant's failure 'to introduce material evidence or to call logical witnesses' is not improper." (*People v. Wash* (1993) 6 Cal.4th 215, 263.) Lund points out that there were innocuous, irrelevant reasons why he might not have called the expert and that it was his counsel's ultimate decision whether to call the expert. This may be true, but it does not negate the prosecutor's right to comment on his failure to call the expert or convert any such comment into an intrusion on attorney-client confidences. If Lund were correct, then prosecutors would be barred from commenting on a defendant's failure to call any witness, which would give defendants an unfair advantage at trial. As the trial court indicated, the prosecutor should have waited to make such commentary in her closing argument rather than introducing the point through her questioning. But because the failure to call a defense expert was a proper subject for prosecutorial comment,

the improper introduction of the concept in Lund's cross-examination was not prejudicial misconduct.

b. Argumentative questioning

Lund's second misconduct argument is more accurately characterized as a subset of his first. Lund contends that the prosecutor engaged in misconduct by continuing to ask argumentative questions even though the trial court repeatedly sustained his objections. "An argumentative question is a speech to the jury masquerading as a question. The questioner is not seeking to elicit relevant testimony. Often it is apparent that the questioner does not even expect an answer. The question may, indeed, be unanswerable." (*People v. Chatman* (2006) 38 Cal.4th 344, 384 (*Chatman*).)

Lund directs us to eight questions and comments he claims are argumentative. Lund did not object to all of these questions, did not always raise the issue of argumentative questioning when he did object, and never raised the issue of misconduct or asked the trial court to admonish the prosecutor to refrain from such questions. However, the trial court stopped the questions even when Lund did not object and twice admonished the prosecutor sua sponte. We will therefore proceed to examine Lund's argument on the merits.

First, after the trial court had sustained his objection to a question and no question was pending, Lund interjected that he couldn't answer the prosecutor's questions because she would not let him read the exhibits. The prosecutor responded, "Do you think you just get to talk when you want to?" Lund did not

object, but the trial court sua sponte admonished the prosecutor, "Don't do that."

Second, the prosecutor asked Lund whether he was aware she had a rebuttal witness coming to contradict his testimony. Lund objected that the question was argumentative, and the trial court sustained the objection, on the basis that the question called for speculation.

Third, after Lund stated that he believed it was unsafe to have computers in patrol cars, despite the CHP policy mandating such computers, the prosecutor asked, "So you know better than all the people that decided that these should go in the CHP patrol cars?" The trial court sustained Lund's objection that the question was argumentative.

Fourth, shortly after asking Lund about a text message he sent in which he described himself as a "neurosurgeon" in comparison to his fellow CHP officers, whom he described as "idiots," the prosecutor asked Lund, concerning a CHP policy he said he was not familiar with, "So you're the neurosurgeon but you never read the policy?" The court sustained the objection that the question was argumentative.

Fifth, after Lund testified that other officers used his desk when he was not in the office, the prosecutor asked, apparently referring to Lund's lack of witnesses corroborating his claims, "Let me guess, you have a witness coming in to say that?" The trial court sustained Lund's objection that the question was argumentative.

Sixth, when Lund told the prosecutor that the pornography in his locker was not his but he did not know who put it there, the prosecutor rejoined, "Okay. You have no answers?" The trial court sua sponte ruled that the question was argumentative.

Seventh, when Lund testified that he could not find a witness to corroborate his claim that another sergeant had a key to his locker because "[i]t's been five years ago," the prosecutor responded, "But it's not been five years since day one." The trial court sua sponte admonished the prosecutor, "We don't need to keep repeating that."

Finally, after Lund admitted that he had been disciplined earlier in his career for viewing pornography on his work computer, the prosecutor asked how many other CHP officers had gotten in trouble for that. Lund objected that the question was argumentative, and the trial court sustained the objection on the grounds of relevance. The prosecutor then asked whether Lund had a "golden" career, referring to a text message in which he had said that. The trial court sustained Lund's objection that the question had been asked and answered.

Lund contends these questions were argumentative and demonstrated the prosecutor's attempt to agitate and belittle Lund to make the jury not like him. Assuming all of the questions were argumentative, only the first question, in which the prosecutor asked whether Lund thought he could talk whenever he wanted, constituted misconduct. That question was not designed to elicit information, or even make an argument to the jury cloaked as a question, but rather aimed to belittle Lund.

However, on its own this single instance of misconduct is de minimis. (*People v. Collins* (2010) 49 Cal.4th 175, 208.) None of the other questions, singly or together, rises to the level of " 'deceptive or reprehensible methods' " that the doctrine of prosecutorial misconduct prohibits. (*People v. Rivera*, *supra*, 7 Cal.5th at p. 333; *People v. Armstrong*, *supra*, 6 Cal.5th at p. 796 ["Effective and legitimate cross-examination may involve assertive and even harsh questioning"].) Despite the questions' sarcastic or biting tone, Lund "identifies no line of questioning, and the transcript reveals none, that crossed over any boundaries of fair play or that would have led the jury to decide this case on anything other than the facts and the law." (*Armstrong*, at p. 96.)

Even if these questions did constitute misconduct, we are satisfied under any standard of prejudice that they did not affect the outcome of the trial. The trial court sustained Lund's objections, dispelling any prejudice. (*People v. Fuiava* (2012) 53 Cal.4th 622, 687.) Additionally, as discussed above, the evidence connecting Lund to the devices containing child pornography was very strong, and the prosecution buttressed it with the striking correspondence between the CPS data and Lund's schedule and movements.

c. Asking whether witnesses were lying

Lund further contends the prosecutor erred by asking him whether other witnesses were lying. Lund objected to only one of the first questions in the prosecutor's series of questions on this topic, on the grounds that it called for speculation and was improper. The trial court overruled the objection. We assume

the objection of impropriety was equivalent to a request for an admonition. Because the court overruled the objection, we conclude any objections to the rest of the questions would have been futile. We will therefore examine Lund's argument on the merits. (*People v. Hill*, *supra*, 17 Cal.4th at p. 820.)

Lund relies on *People v. Zambrano* (2004) 124 Cal.App.4th 228, 242, which held that it is misconduct to ask a defendant if other witnesses are lying where the question serves no evidentiary purpose and serves only to berate the defendant and inflame the passions of the jury.[8] But as *Chatman*, *supra*, 38 Cal.4th at pages 377–384, later made clear, such questions can serve an evidentiary purpose. *Chatman* explained that a "party who testifies to a set of facts contrary to the testimony of others may be asked to clarify what his position is and give, if he is able, a reason for the jury to accept his testimony as more reliable." (*Id.* at p. 382.) The court noted that *Zambrano* had held a prosecutor committed misconduct by asking the defendant whether other witnesses were lying, when the defendant did not know the other witnesses, could not testify about their bias, interest, and motive to be untruthful, and had already contradicted their testimony with his own. (*Id.* at p. 381.) In *Chatman*, by contrast, the prosecutor's questions were proper, because the defendant "was not asked to opine on whether other

[8] Lund also cites *U.S. v. Sanchez* (9th Cir. 1999) 176 F.3d 1214, 1219, which held that asking whether other witnesses are lying is improper because witness credibility is a question for the jury. *Chatman*, *supra*, 38 Cal.4th at pages 380, 382, rejected this principle.

witnesses should be believed" but instead "asked to clarify his own position and whether he had any information about whether other witnesses had a bias, interest, or motive to be untruthful." (*Id.* at p. 383.) The defendant had relevant personal knowledge and knew the other witnesses, who were his friends or relatives. (*Ibid.*)

The prosecutor's questions here fall squarely within the ambit of *Chatman*. The prosecutor did not ask Lund to opine generally on whether the jury should believe the other witnesses, but instead asked more specifically whether he had any reason to believe the other witnesses would make up lies against him. Because Lund took the stand and claimed the witnesses against him were wrong in a way that could only result from deception or bias, it was fair for the prosecution to explore the basis for Lund's belief. This is especially true because Lund worked with many of the witnesses against him and so might have been able to offer some specific testimony regarding any biases or improper motives. Accordingly, the prosecutor's questions about other witnesses do not constitute misconduct.

d. Prosecutor testifying as a witness

Lund argues the prosecutor committed misconduct by testifying as a witness about Duplissey's correction of his report. Lund objected to only two questions in the exchange he cites; he objected that the questions called for hearsay or were leading and called for speculation. Because Lund neither objected to the prosecutor's line of questioning on the ground he now raises nor requested an admonition, he has forfeited this argument. (*People*

v. Prieto, *supra*, 30 Cal.4th at p. 259.) Even were we to consider the argument on the merits, we would reject it because the prosecutor's questions of Duplissey about interactions she had with him are not equivalent to her appearing as a witness.

D. Child pornography videos

Lund's final argument focuses on the child pornography videos the prosecution played for the jury. Lund asserts the prosecution played 50 video segments and argues the prejudicial effect of this evidence substantially outweighed its probative value under Evidence Code section 352. He also asserts the court's decision to admit the evidence without reviewing it in advance was arbitrary. He further argues the admission of this evidence deprived him of a fair trial and violated his right to due process.

"Under Evidence Code section 352, a trial court may exclude otherwise relevant evidence when its probative value is substantially outweighed by concerns of undue prejudice, confusion, or consumption of time. 'Evidence is substantially more prejudicial than probative [citation] if, broadly stated, it poses an intolerable "risk to the fairness of the proceedings or the reliability of the outcome." ' " (*People v. Riggs* (2008) 44 Cal.4th 248, 290.) "In applying this statute we evaluate the 'risk of "undue" prejudice, that is, " 'evidence which uniquely tends to evoke an emotional bias against the defendant as an individual and which has very little effect on the issues,' " not the prejudice "that naturally flows from relevant, highly probative evidence." ' " (*People v. Salcido* (2008) 44 Cal.4th 93, 148.) We review for

abuse of discretion a trial court's decision based on Evidence Code section 352. (*Riggs*, at p. 290.)

Lund's assertion that the prosecutor played 50 video segments is misleading. In response to Lund's motion in limine to exclude the child pornography images and videos, the trial court limited the prosecutor to playing five files from each of the six devices. The prosecutor played even fewer than that, displaying only 15 files to the jury. The prosecutor also skipped ahead quickly in the video files she played for the jury rather than playing entire files. It appears from the record that many video segments were very brief, sometimes a matter of seconds. Lund's approach of counting multiple portions of a single video file as separate video segments would penalize the prosecutor for her apparent attempt to minimize the time spent displaying child pornography. We therefore reject Lund's attempt to inflate the number of videos at issue and will analyze Lund's arguments using the number of 15 child pornography files.

Lund first challenges the files as lacking probative value. He points out that he did not dispute that the files constituted child pornography, merely his knowing possession of them, so he contends the child pornography itself was not probative of his guilt. Lund recognizes the prosecution had to prove that he possessed child pornography, but he maintains the prosecution could have used Datzman's testimony about the videos for this purpose, so the videos were cumulative. We reject these arguments because the law is clear that "the prosecution was not required to accept defense concessions as a sanitized alternative

to the full presentation of its case." (*People v. Zambrano* (2007) 41 Cal.4th 1082, 1149, disapproved on other grounds by *People v. Doolin* (2009) 45 Cal.4th 390.) This is especially true here, where the videos were not merely circumstantial evidence like a crime scene in a murder case, but rather constituted direct evidence of one of the elements of the possession of child pornography charge against Lund. (Pen. Code., § 311.11, subds. (a), (c)(1); *People v. Holford* (2012) 203 Cal.App.4th 155, 171 (*Holford*).) Lund's contention that the videos were unfairly prejudicial by their very nature therefore misses the mark. The relevant question is not whether the prosecution was allowed to show child pornography to the jury, but how much.

On that score, we conclude the trial court did not abuse its discretion in allowing the prosecution to play portions of a few files from each of the electronic devices found to contain child pornography. *Holford*, *supra*, 203 Cal.App.4th 155 is instructive. There, the defendant was charged with possessing a single 25-minute child pornography video. (*Id.* at pp. 158–159.) Without watching the video first, the trial court ruled the entire video was admissible, and the prosecution played all 25 minutes of it for the jury. (*Id.* at pp. 165–166.) On appeal, the court found the video was highly probative because it proved one element of the crime and its length and the obviously young age of the minor in it created an inference that the defendant knowingly possessed it. (*Id.* at pp. 171–173 & fn. 8.) The court further found that while the video was disturbing, "the trial court's determination that the probative value of establishing defendant's knowledge was not

'substantially' outweighed by a 'substantial danger' of prejudice was not arbitrary, capricious nor patently absurd." (*Id.* at p. 174.) The court stated that while it did not condone the practice of ruling on the admissibility of the video without watching it first, the trial court was entitled to rely on an offer of proof and it apparently did so by accepting the parties' agreement that the video was graphic. (*Id.* at pp. 174–175.) The court also noted that the trial court's ruling would have been the same regardless since it reaffirmed its ruling after watching the video. (*Id.* at p. 175.)

In comparison to *Holford*, where there was a single video at issue and the prosecution played all of it, the prosecution's approach here appears to strike a reasonable balance between the potential undue prejudice and the prosecution's desire to present a compelling case. The prosecutor told the court at the hearing before Lund's second trial on Lund's motion to exclude the child pornography that she would follow the same practice that she did at the first, which entailed playing brief portions from up to the first five videos from each device. The trial court estimated the prosecutor spent about 8 to 10 minutes in total displaying photos or videos to the jury in the first trial. The record does not indicate how much time elapsed during the playing of the videos at the second trial, but from the court reporter's transcription of the prosecutor's remarks as she was playing the files, this estimate seems fair. Considering the electronic devices contained thousands of images and videos, eight to ten minutes does not seem excessive, especially because

that total amount of time was broken up into smaller chunks of time for each device.

Lund contends the material issue in *Holford* was whether the defendant knew the video was child pornography, and contrasts that with his defense, which turned only on how the electronic devices came to be found in his locker, desk, and car. He concludes the videos themselves carried little relevance. But as we have noted, the nature of the videos and images as child pornography was still an element of the prosecution's case, and the prosecution was not required to sanitize its case before the jury. The question is one of balance, and Lund does not offer any argument for how much child pornography the prosecution should have been allowed to show, aside from saying that the amount played at trial was too much.

Lund points out that *Holford* suggested its balancing analysis might have come out differently had the defendant been alleged to possess multiple pieces of pornography, like Lund was. (*Holford*, *supra*, 203 Cal.App.4th at p. 171, fn. 7.) *Holford* stated, "[I]n a case involving multiple pieces of child pornography, the probative value of admitting the entirety of a defendant's collection may not be any higher than admitting only a few pieces unless there are other circumstances. Moreover, depending on the depictions in the collection and other circumstances in the case, the danger of prejudice resulting from the admission of an entire collection could substantially outweigh the probative value, particularly since admitting the extra pieces could have

very little effect on the issues given the charging rules for possession of child pornography in California." (*Ibid.*)

These statements are obviously dicta, but they also do not reflect the current state of the law. When *Holford* was decided in 2012, as the court stated, the possession of multiple pieces of child pornography was chargeable as only a single criminal offense. (*Holford*, *supra*, 203 Cal.App.4th at p. 171, fn. 7.) In 2013, the Legislature amended Penal Code section 311.11 to create the separate offense of possession of over 600 child pornography images, more than 10 of which involve a minor under the age of 12, with one video equal to 50 images. (Stats. 2013, ch. 777, § 3.) Now, when a prosecutor is trying to prove such an offense, the display of multiple child pornography images or videos has significant probative value to show a defendant possessed 600 images or 12 videos. Even so, Evidence Code section 352 still plays a role in such cases. The statute does not set any minimum length for a video to qualify as 50 images, so the new offense does not mean a prosecutor can necessarily play the entirety of 12 videos like the 25-minute video at issue in *Holford*. Conversely, a trial court does not necessarily abuse its discretion in allowing a prosecutor to play more than 12 videos, like the prosecutor here, even when the nature of the videos as child pornography is not disputed. The balancing of probative value against the risk of undue prejudice under Evidence Code section 352 remans an issue for the trial court's sound discretion. And under the circumstances here, where the prosecutor displayed one image and portions of 15 videos for what appears to

be a total of approximately eight to ten minutes, we cannot find that the court abused its discretion in striking the balance as it did.

Lund finally argues the trial court abdicated its role as the gatekeeper of evidence by not previewing any of the videos that the prosecution played for the jury, just like the trial court in *Holford*, *supra*, 203 Cal.App.4th at pages 174–175. He contends the trial court's admission of the videos could only have been arbitrary because the prosecution did not even make an offer of proof as to the number of videos, how long the videos were, or the file names of the videos. This argument misconstrues the record. As noted above, the prosecution told the trial court at a pretrial hearing before the second trial that she would limit herself to the first five files from each device, just as she had in the first trial. The record shows the prosecutor did just that. The same judge presided over both trials, and the trials took place only a few months apart, so the trial court was well aware of the nature of the child pornography before the prosecutor played it. Lund quibbles over whether this procedure technically qualified as an offer of proof as to the content of the files, but it amounts to the same thing. The trial court specifically noted that the prosecutor's approach in the first trial was not excessive and she ultimately displayed fewer files to the jury than the trial court had authorized. The second trial was similar, with the prosecution displaying 15 videos and one image to the jury, not the full 30 files authorized by the trial court's ruling. Because the trial court had already seen the videos that would be played,

its decision was "an informed one and not ' "a shot in the dark." ' " (*Id.* at p. 174.) The trial court did not abdicate its role.[9]

III. DISPOSITION

The judgment is affirmed.

BROWN, J.

WE CONCUR:

POLLAK, P. J.

STREETER, J.

People v. Lund (A157205)

[9] The only error that Lund has shown in his trial was the de minimis misconduct of one improper statement by the prosecutor. As a result, we need not consider Lund's contention that the cumulative effects of multiple errors in his trial made it fundamentally unfair in violation of due process.

Trial Court: Solano County Superior Court

Trial Judge: Hon. Daniel J. Healy

Counsel:

Law Offices of Beles & Beles, Robert J. Beles, Joseph L.Ryan, for Defendant and Appellant.

Xavier Becerra, Attorney General, Lance E. Winters, Chief Assistant Attorney General, Julie L. Garland, Assistant Attorney General, A. Natasha Cortina, Annie Featherman Fraser, Deputy Attorneys General, for Plaintiff and Respondent.