Filed 2/1/17 P. v. Zuniga CA2/2

**NOT TO BE PUBLISHED IN THE OFFICIAL REPORTS**



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

| | |
|---|---|
| THE PEOPLE,<br><br>Plaintiff and Respondent,<br><br>v.<br><br>ANDREW ZUNIGA,<br><br>Defendant and Appellant. | B266744<br><br>(Los Angeles County Super. Ct. No. KA104774) |

APPEAL from a judgment of the Superior Court of Los Angeles County. Rogelio Delgado, Judge. Affirmed.

Kevin D. Sheehy, under appointment by the Court of Appeal, for Defendant and Appellant.

Kamala D. Harris, Attorney General, Gerald Engler, Chief Assistant Attorney General, Lance E. Winters, Assistant Attorney General, Stephanie A. Miyoshi and Allison H. Chung, Deputy Attorneys General, for Plaintiff and Respondent.

Defendant and appellant Andrew Zuniga (defendant) appeals from his conviction of possession of child pornography. He contends that the trial court erred in failing to give a sua sponte instruction on an affirmative defense, and that the trial court erred in denying his motion for acquittal based on insufficient evidence. Finding no merit to defendant's contentions, we affirm the judgment.

## BACKGROUND

Defendant was charged with possession of child pornography, in violation of Penal Code section 311.11, subdivision (a).[1] The information further alleged that defendant had been convicted of a serious or violent felony within the meaning of the "Three Strikes" law (§§ 667, subd. (b)-(i) & 1170.12), as well as a prior conviction and prison term within the meaning of section 667.5, subdivision (b). The prior conviction allegations were bifurcated, defendant waived his right to trial on the allegations, and admitted them. After a jury found defendant guilty as charged, the trial court sentenced defendant to a total prison term of five years, comprised of the middle term of two years, doubled as a second strike, plus one year pursuant to section 667.5 subdivision (b), with presentence custody credits of 184 days. The court ordered defendant to pay mandatory fines and fees and to register as a sex offender.

Defendant filed a timely notice of appeal from the judgment.

---

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

**Prosecution evidence**

Defendant, a parolee subject to search conditions, was searched by parole agents at their offices on February 19, 2014. On the Apple iPhone recovered from defendant, agents found the three photographs that gave rise to the criminal charge against defendant. After defendant admitted the cell phone was his, the police were called and defendant was taken into custody. El Monte Police Officer Aran Choe took possession of the cell phone at the parole office. He accessed the photographs by pressing the icon for an application called "Photos," which opened to a page with a series of sub-folders, one of which was marked, "Photo Stream." There, Officer Choe found the three photographs, along with many personal photographs of defendant.

One of the three subject photographs depicted a topless girl who appeared to be between five and seven years old, with an adult penis near her face, apparently resting on her chin. The second photograph depicted a toddler or a child of four to six years of age, lying on her stomach or side, with what appeared to be adult female hands spreading the buttocks open, exposing the anus and genitals. The third photograph depicted a girl who appeared to be between seven and nine years old, wearing a halter top, with her underwear pulled down, and an eight to ten-year-old boy with his mouth pressed against the girl's genitals.[2]

---

[2] There may have been a fourth photograph that disappeared when the data was later extracted from the cell phone, as one of the parole agents, Stanley Tate, testified that none of the three photographs in evidence at trial was the one he saw. He described a photograph similar to the one depicting a little girl and an adult penis.

Los Angeles Police Detective Shannon Geaney, the supervisor of the forensic computer lab for the Internet Crimes against Children Task Force, testified as the prosecution's expert in forensic examination of electronic devices capable of storing digital media, including computers, cameras, and cell phone. She examined defendant's iPhone, extracted the data and created digital reports, using software programs Lantern and Cellebrite. Programmed into the phone were the phone's name, "Andrew's Phone," as well as the email addresses, "andrew_zun@yahoo.com," and "andrew_zun@icloud.com."

Among the photographs extracted from defendant's iPhone were the three subject photographs depicting child pornography. Detective Geaney explained how iPhones saved and stored photographs. There are three steps required for saving photographs attached to messages: (1) opening the email or text; (2) pressing on the image, which then gives the user the option to save, copy, cancel, or sometimes share; and then, (3) pressing save. The photographs taken by the user's phone or saved directly to the phone by the user are contained in the Camera Roll, where they remain in a photo gallery and may be copied into separate Album folders. The Camera Roll contains thumbnail images, and another copy is created as a large image that will appear when the user presses the thumbnail image. Apple iCloud is a service that allows data storage on Apple's servers and which can synchronize data among more than one device operated by "iOS," the Apple operating system. To save photographs in the Photo Stream, a user must first save the photograph to the cell phone, at which time a copy is automatically created and sent to the Photo Stream, where it is archived until deleted. A photograph manually saved by the user

will remain in the cell phone's memory until deleted, and if it is deleted from the cell phone's memory, it will remain in the Photo Stream for 30 days unless consciously deleted from that location as well.

The photographs stored in the Photo Stream may be shared with others by means of email, text messaging, or the internet. As defendant's account was the only iCloud account associated with defendant's cell phone, he was the only person who could store images there unless he set it up to accept outside data, which he had not done. Thus, in order to share photographs, a separate folder or Album would have to be created for that purpose. No separate Album had been created on defendant's cell phone, and Detective Geaney found no indication that defendant had shared any of his photographs. This meant that the three pornographic photographs had been either downloaded from the internet or received via email or text message and then saved to defendant's cell phone.

Detective Geaney determined that the first of the three photographs was saved to defendant's iPhone on January 31, 2014. The second and third photographs were saved to defendant's iPhone on February 4, 2014. Although her analysis showed that texts and emails were received and sent during the period before January 31, 2014, through February 3, and that some photographs had been received in messages, she could not determine where they originated or which messages contained photographs, because the call log had been deleted. Detective Geaney explained that iOS tracks only the date the photograph or file was first created when the user saved it on the phone. Files cannot be modified, but the user must instead create a new file with the changes and assign it a new name. Cellebrite

software generates a report capable of showing created, modified, and accessed dates, only because some other devices are capable of tracking that information. When the device is an Apple device, the Cellebrite report states the date the file was created, and then simply repeats the same date in the remaining two categories. The modified and accessed dates are thus unreliable and irrelevant, and it is Detective Geaney's practice to eliminate those categories from the iPhone reports she prepares.

In Detective Geaney's opinion, the three photographs were saved from either a website, a text, or an email to the Camera Roll's photo gallery; the program then automatically duplicated them into the Photo Stream, and they remained there after the entries in the Camera Roll were deleted. All three images of child pornography extracted from defendant's iPhone had been stored in the same Photo Stream file path that also included hundreds of defendant's personal photographs. The three pornographic images were located at the top of the gallery view and were immediately followed by Defendant's personal photographs. In Detective Geaney's opinion, it was not possible for photographs to appear inadvertently in the Photo Stream; an iPhone user must consciously save photographs in the phone in order for them to appear in the Photo Stream. In her experience, Detective Geaney had never known an image to be sent to the Photo Stream without a deliberate decision made by the iPhone's user to save it. Hacking an iCloud account is possible but extraordinarily unlikely, as Apple's servers are very secure. There would be no record in the phone that the Photo Stream was accessed, and Detective Geaney found no evidence that defendant's Photo Stream had been accessed.

**Defense evidence**

Mark Joseph Eskridge, a former police officer and district attorney investigator, was a private investigator specializing in forensic computer and cell phone examination who testified as defendant's expert. Eskridge ran Cellibrite and Lantern analyses on defendant's iPhone, and found that defendant had an easy-to-guess password for iCloud, "Drew1234," created from his name. Eskridge testified that with a password, a cell phone can be remotely accessed to upload data from or download data to an iCloud account.

Eskridge also testified that Apple experienced security problems in 2013 and 2014, explaining that celebrity photos were stolen from Apple accounts by means of the "iBrute" software designed by hackers to automatically and quickly try possible passwords until one worked. Apple changed its security protocols in 2014 to eliminate the problem by adding lockout and notification features to its iCloud application, and iPhones are now more secure. Since Apple's 2014 security improvement, there has been no other iBrute hack, and Eskridge knew of no other such vulnerability in Apple's servers.

Eskridge testified that photographs cannot appear in a photo gallery or Photo Stream just because an email or text was sent to the iPhone; the user must deliberately save any attached image. Deleting a message without accessing and saving the image would delete the photograph with it, and it would not be stored. Since the Photo Stream function was activated on defendant's cell phone, saved data would be accessible from any synched device, but Eskridge saw no indication of another device having been synched to defendant's iPhone. Deleting a saved photograph from the iPhone would not delete the copy in the

Photo Stream, where it would remain for at least 30 days. Photographs appear in the gallery by date saved, with the newest at the bottom. Eskridge found no evidence that defendant had ever personally accessed anything on the Photo Stream, and furthermore he had never heard of any instances where information was placed into a hacked account.

## DISCUSSION

### I. Momentary possession defense

Defendant contends that the trial court erred in failing to give a sua sponte jury instruction regarding the affirmative defense of momentary possession, which was recognized as a defense to possession of narcotics in *People v. Mijares* (1971) 6 Cal.3d 415 (*Mijares*). *Mijares* "held that, under limited circumstances, momentary or transitory possession of an unlawful narcotic for the sole purpose of disposing of it can constitute a defense to a charge of criminal possession of the controlled substance. [Citation.]" (*People v. Martin* (2001) 25 Cal.4th 1180, 1182, citing *Mijares*, at p. 419.) The *Mijares* defense has been extended to the possession of a firearm by a felon (see *People v. Hurtado* (1996) 47 Cal.App.4th 805, 814). The California Supreme Court has indicated that the defense may be available to a charge of possessing child pornography in violation of section 311.11, subdivision (a). (*In re Grant* (2014) 58 Cal.4th 469, 478-479.) The defense would "cover[] a person who innocently receives unsolicited material, discovers it contains child pornography, and immediately destroys the material or reports it to law enforcement . . . ." (*Id*. at p. 479.) The *Mijares* defense requires proof that the defendant had only a "'fleeting, de minimus possession and a reflexive act of abandonment.'" (*People v. Martin*, *supra*, 25 Cal.4th at p. 1188.)

A trial court has a sua sponte duty to instruct on a defense only if the defendant appears to rely on the defense, or if there is substantial evidence supporting the defense and it is not inconsistent with the defendant's theory of the case. (*People v. Breverman* (1998) 19 Cal.4th 142, 157-158; *People v. Barton* (1995) 12 Cal.4th 186, 195.)

Based on these authorities the trial court was required to instruct sua sponte when there is substantial evidence that defendant had possession of the three photographs, that possession was unsolicited, and that defendant immediately deleted the photograph after seeing what it was, and the defense was not inconsistent with the defendant's theory of the case.

Defendant contends that substantial evidence supports an inference that he did not solicit the photographs and that he immediately deleted them, as shown by the following evidence: the phone contained only three pornographic photographs of children among hundreds of personal photographs; the three photos were saved on just two days, January 31 and February 4; and the photographs were deleted, as they were no longer on the Camera Roll when they were discovered in the Photo Stream on February 19. Defendant also argues that because the Cellebrite program reported an identical created, modified, and accessed date, this suggested that the photographs were deleted on the same day they were saved. In addition, defendant points to the *absence* of evidence, or any forensic method of obtaining evidence, that defendant had personally solicited any of the three photographs or downloaded them from the internet, or that defendant had ever accessed or viewed any of the three photographs from the Photo Stream after they were first viewed and deleted from the Camera Roll.

As defendant argues, in determining whether a sua sponte instruction was required, we view the evidence in the light most favorable to the defendant. (See *People v. Millbrook* (2014) 222 Cal.App.4th 1122, 1137 [lesser included].) However, the evidence must be substantial, not simply "'*any* evidence, no matter how weak.'" (*People v. Breverman*, *supra*, 19 Cal.4th at p. 162.) And of course, an absence of evidence is not substantial evidence, as "'[a] party is not entitled to an instruction on a theory for which there is no supporting evidence.' [Citation.]" (*People v. Tufunga* (1999) 21 Cal.4th 935, 944.) The Cellebrite program did not report the modified and accessed dates of the photographs, as defendant asserts, because defendant's iPhone did not track such dates. The report merely entered the created/saved date, and then repeated it twice. There was no evidence, favorable or unfavorable to defendant, as to when, during the more than two weeks after the photographs were first saved until discovered by law enforcement, they were deleted from the Camera Roll. Thus, the only actual evidence remaining in defendant's summary is that only three photographs depicting child pornography were among hundreds of other photographs discovered on defendant's phone, that the three photographs were saved on the Camera Roll on January 31 and February 4, and that they were afterward deleted from that folder on a date before February 19.

Such facts may give rise to a reasonable inference that it was defendant who saved and then deleted the photographs; however, they provide no evidence of when defendant deleted the photographs. It might have been immediate, or it might have been two weeks later. That is an insufficient basis upon which to require a sua sponte instruction. (*People v. Wilson* (1992) 3 Cal.4th 926, 942.)

Moreover, the *Mijares* momentary possession defense is inconsistent with the defense theory at trial that defendant never knowingly had possession of the three photographs. Fleeting possession is still possession, and having a purpose is a conscious thought; thus, there cannot be possession for the sole purpose of disposal without a knowing possession. Defendant did not testify, instead his evidence consisted of expert testimony regarding ways that iCloud could be hacked and material downloaded into the Photo Stream. In summation, defense counsel first noted that it was common knowledge that individuals and large corporations were victims of hacking, the theft of data and passwords, and the placement of harmful data on devices. Counsel argued that there was no evidence that defendant knew the photographs were in his phone or that he deleted them. After paraphrasing Detective Geaney's testimony that there was no deletion date on the report or any indication that the photographs were accessed or viewed from the Photo Stream, counsel urged the jury to find a reasonable doubt as to whether defendant ever saw the photographs or personally deleted them. Counsel argued that just because the cell phone was in defendant's "pocket 24 hours a day . . . doesn't mean he could control everything that comes onto the phone."

Defendant acknowledges that the overarching defense theory was that there was no evidence that defendant took the photographs or that he solicited, accessed, saved, or tried to delete them. However, to demonstrate that a momentary possession defense was not inconsistent with the defense theory, defendant points to the following parts of defense counsel's summation, where counsel described the prosecution theory:

> "When someone sends you an e-mail, you don't know it's there until it's there, and it is there, essentially, forever. Why do I say 'It is there forever?' Because -- and I thank Detective Geaney for this -- we may think we delete things. You get an advertisement on your cell phone and you say, 'I don't need this,' and you hit delete and it's gone. It isn't gone. It is still there, only you can't access it, and I am building a great portion of the defense in this case upon precisely what Detective Geaney had to say, 'It is there.'"
>
> "I believe Detective Geaney's theory, and that's all it was, a theory, is that my client saw something, maybe accessed a porn site, saw some kiddie porn and said, 'Gee, I like that,' downloaded it. Unbeknownst to him, once he did that, boom, it goes over to the Cloud, but he's still on the phone side, and what does he say? . . . 'I'm gonna get rid of it now.' Boom, it's deleted, but you know what, . . . it isn't deleted."

Defense counsel went on to argue that the evidence did not support Detective Geaney's theory, and in particular, that the evidence did not show that defendant knew the photographs were in his phone. There is nothing in these excerpts suggesting a theory that defendant accessed the photographs, did so for the purpose of deleting them, and deleted them immediately.

In sum, there was no substantial evidence that the deletion of the photographs was immediate, and the defense theory was inconsistent with a *Mijares* momentary possession defense, as counsel argued that defendant did not view the photographs and did not personally delete them, or even have knowledge of their existence on his cell phone. Under such circumstances, the trial

court had no sua sponte obligation to instruct with regard to a momentary possession defense. (See *People v. Breverman*, *supra*, 19 Cal.4th at pp. 157-158;*In re Grant*, *supra*, 58 Cal.4th at pp. 478-479.)

**II. Substantial evidence of knowing possession**

Defendant contends that no substantial evidence supported the knowledge element of the offense, and that the trial court erred in denying his motion for acquittal, brought pursuant to section 1118.1.[3]

We independently review a trial court's ruling under section 1118.1 that the evidence is sufficient to support a conviction, and apply the same substantial evidence test. (*People v. Cole* (2004) 33 Cal.4th 1158, 1212-1213.)[4] "[W]e review the entire record in the light most favorable to the judgment to determine whether it discloses substantial evidence -- that is, evidence that is reasonable, credible, and of solid value -- from which a reasonable trier of fact could have found the defendant

---

[3] Section 1118.1 provides in relevant part: "In a case tried before a jury, the court on motion of the defendant or on its own motion, at the close of the evidence on either side and before the case is submitted to the jury for decision, shall order the entry of a judgment of acquittal of one or more of the offenses charged in the accusatory pleading if the evidence then before the court is insufficient to sustain a conviction of such offense or offenses on appeal."

[4] "'Where the section 1118.1 motion is made at the close of the prosecution's case-in-chief, the sufficiency of the evidence is tested as it stood at that point.' [Citations.]" (*People v. Cole*, *supra*, 33 Cal.4th at p. 1213.) Here, the motion was made after both sides rested, the jury had been instructed, and just before the prosecutor's final argument. We thus review all the evidence.

guilty beyond a reasonable doubt. [Citations.]" (*Id*. at p. 1212; see also *People v. Johnson* (1980) 26 Cal.3d 557, 578; *Jackson v. Virginia* (1979) 443 U.S. 307, 318-319.) We begin with the presumption that the evidence was sufficient. (*People v. Sanghera* (2006) 139 Cal.App.4th 1567, 1573.) And "we must . . . presume in support of the judgment the existence of every fact the trier could reasonably deduce from the evidence. [Citation.]" (*People v. Jones* (1990) 51 Cal.3d 294, 314.) "The same standard applies when the conviction rests primarily on circumstantial evidence. [Citation.]" (*People v. Kraft* (2000) 23 Cal.4th 978, 1053.) "An appellate court must accept logical inferences that the jury might have drawn from the circumstantial evidence. [Citation.]" (*People v. Maury* (2003) 30 Cal.4th 342, 396.) Reversal on a substantial evidence ground "is unwarranted unless it appears 'that upon no hypothesis whatever is there sufficient substantial evidence to support [the conviction].' [Citation.]" (*People v. Bolin* (1998) 18 Cal.4th 297, 331.)

Section 311.11, subdivision (a), prohibits knowingly possessing or controlling any image of child pornography. Defendant contends that knowing possession or control is missing here because there was *no* evidence that defendant had personally "ever (even momentarily or fleetingly) solicited, viewed, accessed, or saved any of the three photos on the cell phone," or evidence that he had accessed or viewed the images saved in the Photo Stream or other device.

Defendant's claim lacks merit. Both experts testified that the iPhone user must consciously save a downloaded image or one attached to an email or text for it to be duplicated into the Photo Stream. Eskridge testified that deleting a message without accessing and saving the image would delete the

photograph with it, and it would not be stored. Further, as respondent argues, the fact that three pornographic photographs were saved on two different dates suggests a pattern of deliberate conduct. Thus, for the images to be saved in the iCloud Photo Stream, *someone* had to either download them from the internet, or open an attachment and consciously save the images to the Camera Roll. Only then would the images be automatically duplicated into the Photo Stream, unless the Photo Stream had a shared gallery, which defendant's Photo Stream did not have.

Quoting from *Tecklenburg v. Appellate Division* (2009) 169 Cal.App.4th 1402, 1413 (*Tecklenburg*), defendant argues that simply being the registered owner of the electronic device containing child pornography "'would not be sufficient alone to show he was the person who had entered the word searches or Web site addresses or accessed the Internet images and graphics found on'" the device. In *Tecklenburg*, however, the electronic device in question was a family computer, shared by the defendant, his two sons, and two or more daughters; thus, the issue discussed in the quoted excerpt was which of those persons had accessed the child pornography. (See *id.*, at pp. 1411-1413.) Here, there was no evidence of other users of defendant's iPhone, and the Cellebrite analysis revealed no other iCloud account, no sharing of data, and no indication that other devices were synched to the account.

Moreover, the evidence did not merely show that defendant was the registered owner of the iPhone. Defendant admitted ownership of the phone, and the phone was programmed with the name, "Andrew's Phone," as well as with email addresses based on defendant's name. Such facts, plus the fact that the phone was found on defendant's person, gave rise to the reasonable

inferences that the cell phone was defendant's personal phone, that he had sole access to it, and that he was thus the person who saved the images to the Camera Roll.[5] We thus reject defendant's contention that the evidence gave rise only to suspicion and speculation that defendant was the person who accessed the photographs on his cell phone, saved them, and then deleted them from the Camera Roll.

Defendant suggests that the evidence of accessing and saving prohibited images is necessarily insubstantial unless it is as extensive as in some other cases, such as *Tecklenburg* and *People v. Mahoney* (2013) 220 Cal.App.4th 781, 794-795, where images were found on multiple electronic devices owned or controlled by the defendant, or where hundreds of images of child pornography were found, or there was evidence of multiple internet searches for child pornography. "When we decide issues of sufficiency of evidence, comparison with other cases is of limited utility, since each case necessarily depends on its own facts. [Citation.]" (*People v. Thomas* (1992) 2 Cal.4th 489, 516.) Moreover, the cited cases did not establish a minimum number of photographs or searches that must be proven; nor did they hold that the appellate court may not affirm a child pornography conviction unless the evidence was overwhelming. "'[I]t is the

---

[5] Evidence that defendant knew that the photographs had been automatically duplicated into the Photo Stream was unnecessary. Knowing possession or control of child pornography may be proven by the deliberate downloading and saving such material to a computer, without having to show that the defendant was aware of an automatic storage in the computer's cache files. (*Tecklenburg, supra*, 169 Cal.App.4th at p. 1419 & fn. 16.)

jury, not the appellate court which must be convinced of the defendant's guilt beyond a reasonable doubt.'" (*Id.* at p. 514.)

We conclude substantial evidence supported reasonable inferences that defendant was the person who accessed and then deliberately saved the photographs on the iPhone's Camera Roll, and thus knowingly controlled the images. For the same reason, we also conclude that the motion for acquittal was properly denied.

**DISPOSITION**

The judgment is affirmed.

NOT TO BE PUBLISHED IN THE OFFICIAL REPORTS.

_____, Acting P. J.
CHAVEZ

We concur:

_____, J.*
GOODMAN

_____, J.
HOFFSTADT

---

*Retired Judge of the Los Angeles Superior Court, assigned by the Chief Justice pursuant to article VI, section 6 of the California Constitution.