NOT TO BE PUBLISHED IN THE OFFICIAL REPORTS

California Rules of Court, rule 8.1115(a), prohibits courts and parties from citing or relying on opinions not certified for publication or ordered published, except as specified by rule 8.1115(b). This opinion has not been certified for publication or ordered published for purposes of rule 8.1115.

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA

SECOND APPELLATE DISTRICT

DIVISION ONE

THE PEOPLE,

Plaintiff and Respondent,

v.

BRADLEY HARLAN FIELD,

Defendant and Appellant.

B290692

(Los Angeles County Super. Ct. No. BA456917)

APPEAL from a judgment of the Superior Court of
Los Angeles County, Sergio C. Tapia II, Judge. Affirmed.
Richard D. Rome for Defendant and Appellant.
Xavier Becerra, Attorney General, Gerald A. Engler,
Chief Assistant Attorney General, Lance E. Winters, Assistant
Attorney General, Paul M. Roadarmel, Jr., and Kristen J. Inberg,
Deputy Attorneys General, for Plaintiff and Respondent.

A jury convicted Bradley Harlan Field of one count of possession of child pornography, in violation of Penal Code section 311.11, subdivision (a). The jury also found that Field possessed more than 600 images of child pornography, including at least 10 images of a prepubescent minor or a minor under 12 years of age. (§ 311.11, subd. (c)(1).) The trial court sentenced Field to 36 months of formal probation, one of the terms of which was to serve 120 days in county jail.

Field challenges his conviction, contending that the trial court abused its discretion by allowing the admission of evidence from a copy of his computer's hard drive that he contends was hearsay and was not properly authenticated. He also contends that the court erred by denying his *Trombetta*² motion to dismiss the case because prior to trial, the Los Angeles County Sheriff's Department destroyed evidence that Field claims was vital to his defense. We affirm.

FACTS AND PROCEEDINGS BELOW

On March 19, 2016, Field bought a used Dell laptop computer from Fry's Electronics in Oxnard. About four months later, on August 4, he found that the computer would no longer turn on, so he took it to Pacific Computers in Calabasas for repairs. A store employee ran diagnostic tests and determined that the laptop's hard drive was failing. Because the laptop was relatively old, an employee recommended that Field buy a new computer rather than repair his existing one. The store could still salvage the files from the failing hard drive by transferring

¹ Unless otherwise specified, subsequent statutory references are to the Penal Code.

² California v. Trombetta (1984) 467 U.S. 479 (Trombetta).

them to a USB flash drive. Field agreed, but insisted that the defective hard drive be completely destroyed after the data transfer was complete. When the hard drive was connected to the store's computer to complete the transfer, an employee noticed that some of the files on Field's hard drive had names suggesting that they might contain child pornography. The technician called the store's owner, who logged into the store's computer system remotely and opened some of the files. The owner determined that the files indeed contained child pornography and called the Los Angeles County Sheriff's Department.

The following day, Nestor Cienfuegos, a deputy sheriff, was dispatched to the store. Field's laptop was still connected to the store's computer, which displayed the names of the files from Field's hard drive. Deputy Cienfuegos clicked on one of the files and verified that it appeared to contain sexually explicit images of children. He then took custody of the laptop and flash drive and booked them into evidence at the sheriff's station in Lost Hills.

Bernell Trapp, a detective with the sheriff's department, interviewed Field at his home on August 5, 2016, the same day the deputies took the laptop into custody. Field told him that the laptop came with Windows 7 installed when he bought it used from Fry's Electronics a few months earlier. Field said he used the computer for his work as an attorney and occasionally viewed gay adult pornography on it. He denied knowing about any child pornography on the computer. He said that a couple of friends sometimes used his computer, but he did not believe they would have downloaded child pornography on it.

Aaron King, a detective with the sheriff's department who specializes in high tech crimes, examined the laptop shortly after Deputy Cienfuegos booked it into evidence. Detective King could not turn the computer on, but he removed the hard drive and was able to make an exact copy of it on the sheriff's department computer system.³ Approximately eight months later, in April 2017, Detective King searched the image of the hard drive and determined there was a folder labeled "KP VIDS" containing 34 videos and images of child pornography. Detective King determined that the "KP VIDS" folder was located in the folder with downloads of a user labeled "B. Harlan Field." In the summer of 2017, Detective King again searched the image of the hard drive and determined that there were 835 images of child pornography in a folder labeled "KP RAR." The KP RAR folder was also located in the downloads folder of user B. Harlan Field. The file names of the documents within all of these folders strongly suggested that they depicted child pornography. The downloads folder also contained several documents pertaining to the practice of law, which was Field's profession. These included one page with Field's name on it labeled "verification" that appeared to come from a blank pleading in a lawsuit. B. Harlan Field was the only user profile name on the computer. The metadata of the hard drive showed that all the child pornography files were downloaded between June 21, 2016

³ As we explain in more detail below (see Discussion part II.A, *post*), an error in the classification of the case in the sheriff's department computer system caused the department's central property and evidence unit to destroy Field's laptop in July 2017. The prosecution relied on the copy of the hard drive rather than the original hard drive as evidence against Field.

and July 9, 2016. The hard drive also contained several ".lnk" shortcut files linking to the child pornography files, which suggested that many of the child pornography images and videos had been accessed or opened within the same dates. The metadata also indicated that the Windows 7 operating system had been installed on the laptop on March 19, 2016, and that the registered owner was B. Harlan Field. March 19, 2016 was the same date Field purchased the laptop.

The prosecution and defense agreed to the following stipulation, which was read to the jury: "The parties stipulate that the images and/or video found on the laptop computer . . . depict a person under the age of 18 years of age personally engaging in or simulating sexual conduct and the matter contains more than 600 images that violate . . . section 311.11[, subdivision](a), including ten or more images of a prepubescent minor or a minor who was under 12 years of age."

Field testified in his own defense. He acknowledged having purchased the used laptop from Fry's Electronics in Oxnard. Field also acknowledged that he installed Windows 7 on his computer when he bought it, and entered the user name "B. Harlan Field." He denied knowing that there was child pornography on the computer. He claimed that a woman named Alaina, who lived in the same apartment complex in Malibu where Field lived sometimes visited and used Field's computer. Field could not see what Alaina was doing on his computer because she visited websites written in the Cyrillic alphabet. Field described Alaina as a woman in her mid-30's with red hair who spoke with a Russian accent, but he did not know her last

name. According to Field, she moved away in 2017, a year before the trial.

DISCUSSION

A. Hearsay and Authentication

Field contends that the trial court abused its discretion by admitting evidence pertaining to the user profile name "B. Harlan Field" on his computer. He argues that this evidence was inadmissible hearsay and that it was not properly authenticated. We disagree.

1. Hearsay

When the sheriff's deputies examined the copy of Field's hard drive, they discovered that the child pornography was in a file directory associated with a user account labeled "B. Harlan Field." At trial, the prosecution sought to introduce as evidence printouts from Field's computer, which included the profile name "B. Harlan Field" as part of the file path. The defense filed a motion under Evidence Code section 402 to exclude the evidence, arguing that the account name "B. Harlan Field" was hearsay, and that it was being offered for the truth of the matter asserted. The trial court denied the motion, finding that the user name and associated documents were admissible as circumstantial evidence linking Field to the computer.

⁴ At the time the trial court made its ruling on the hearsay issue, Field had not yet testified in his own defense. During his testimony, he acknowledged that he created and used the B. Harlan Field account. The trial court did not address the prosecution's argument that the account name was also admissible under the hearsay exception for admissions by a party. (See Evid. Code, § 1220.)

The court allowed the prosecution to introduce the evidence subject to a limiting instruction. When Detective King testified about finding child pornography in an account under the name B. Harlan Field, the court instructed the jury that the user name was "not being introduced to indicate that the gentleman that's here in court is the same person in the user profile."

Field argues that the court abused its discretion by allowing the testimony about the user profile name. He contends that the evidence was in fact inadmissible hearsay because the prosecution used it to prove the truth of the matter asserted. We need not decide whether the evidence was offered for the truth of the matter asserted because even if so, it was admissible under the hearsay exception for statements offered against the declarant, as codified in Evidence Code section 1220.

If a defendant's own statements are offered against him at trial, "the hearsay rule does not make the statements inadmissible." (*People v. Carpenter* (1990) 21 Cal.4th 1016, 1049; Evid. Code, § 1220.) In this case, a great deal of circumstantial evidence supported the conclusion that Field himself created the B. Harlan Field user profile name. According to Detective King, the account was created on March 19, 2016, the same date Field purchased the computer, almost immediately after the Windows 7 operating system was installed on the computer. Field told Detective Trapp in an interview the day after the child pornography was discovered that he lived alone and that the only other users of the computer were a couple of friends whom Field occasionally allowed to use it. "[U]nder the circumstances, the court and, ultimately, the jury could readily find that defendant did" create the user name. (*People v. Becerrada* (2017) 2 Cal.5th

1009, 1025.) "Indeed, it is hard to imagine who, other than defendant, might have" done so.⁵ (*Ibid.*)

So long as there is one legal theory supporting the trial court's ruling to admit evidence, we may affirm it regardless of whether the court's stated reasoning was correct. (See *People v. Horning* (2004) 34 Cal.4th 871, 898; *People v. Zapien* (1993) 4 Cal.4th 929, 976.)

2. Authentication

Written documents must be properly authenticated before they can be admitted in evidence. (Evid. Code, § 1401; People v. Goldsmith (2014) 59 Cal.4th 258, 266 (Goldsmith).) This rule applies to words recorded tangibly in any medium, including those stored electronically. (See Evid. Code, § 250; People v. Dawkins (2014) 230 Cal. App. 4th 991, 1002.) Authentication requires that the proponent introduce evidence "sufficient to sustain a finding that it is the writing that the proponent of the evidence claims it is." (Evid. Code, § 1400.) Thus, writing is admissible as long as the trial court finds that a factfinder can find by preponderance of the evidence that the writing is authentic. (Goldsmith, supra, 59 Cal.4th at p. 267–268.) There are no restrictions on "the means by which a writing may be authenticated." (Evid. Code, § 1410.) A party may rely on "other witness testimony, circumstantial evidence, content and location." (Goldsmith, supra, 59 Cal.4th at p. 268.) If conflicting inferences can be drawn regarding authenticity, that

⁵ We reach this conclusion without relying on Field's subsequent trial testimony during which he admitted that he created the user account.

consideration "goes to the document's weight as evidence, not its admissibility." (*Id.* at p. 267.)

In this case, the prosecution introduced several documents that it alleged were printouts from the image of Field's hard drive, showing the installation date of Windows 7, the creation date of the B. Harlan Field user account, the contents of the downloads directory of that user account, and the creation date of various subfolders and documents within the downloads directory. In his testimony, Detective King described how he copied Field's hard drive into an image that was stored within the sheriff's department computer system, as well as how each of the printouts accurately reflected the contents of the hard drive image.

Field contends that this did not meet the standard of authentication to allow for admission of the documents into evidence. He argues that Detective King's testimony was insufficient to connect the B. Harlan Field user account and the documents in it to Field himself. But that was not required. The prosecution needed to show only enough to allow "a trier of fact to find that the writing is what it purports to be." (Goldsmith, supra, 59 Cal.4th at p. 267.) In this case, the writings purported to be copies of documents from the image of Field's hard drive, and Detective King's testimony allowed the jury to conclude just that. The issue of whether Field actually created the B. Harlan Field user account and downloaded child pornography into that user account was a separate question for the jury to decide.6

⁶ Because we deny Field's argument on the merits, we need not decide whether he properly preserved the argument on appeal.

For the first time in his reply brief, Field contends that the trial court should have excluded evidence pertaining to the B. Harlan Field user account pursuant to Evidence Code section 352 because the potential prejudicial effect of the evidence greatly outweighed its probative value. Field forfeited this argument by failing to raise it in his opening brief on appeal. (See People v. Baniqued (2000) 85 Cal.App.4th 13, 29 [an argument withheld until a reply brief "is deemed waived and will not be considered, unless good reason is shown for failure to present it before"].) In addition, the argument fails on the merits. For purposes of Evidence Code section 352, evidence is prejudicial not because it is damaging to the opposing party, but because it is likely to cause the jury to disregard logic and "' "to reward or punish one side because of the jurors' emotional reaction." '" (People v. Bell (2019) 7 Cal.5th 70, 105.) Under this standard, there was nothing prejudicial about introducing the user profile name.

B. Trombetta Motion

Field contends that the trial court erred by denying his *Trombetta* motion to exclude evidence against him that the police destroyed prior to trial. He argues that this evidence was vital to his defense, and that the court violated his right to due process by allowing the case to continue after its destruction. We disagree.

1. Factual Background

Field's laptop computer and the USB flash drive onto which the Pacific Computers employees copied the contents of his hard drive were destroyed in the custody of the sheriff's department before trial. According to sheriff's department employees, this destruction was accidental and the result of a misunderstanding by sheriff's deputies regarding the department's policies for the retention of evidence.

Kenneth Howard, a criminalist with the sheriff's department who manages the department's PRELIMS system for managing evidence testified that the sheriff's department policy is to retain evidence pertaining to felony cases indefinitely, but to dispose of evidence in misdemeanor cases after six months. Whenever a sheriff's deputy opens a new case, the sheriff's department computer system generates a 15-digit number called a URN to identify the case. The first digit is known as a retention code, and the remaining digits refer to the year when the case was opened, the location where the alleged crime took place, the station handling the case, the sequential number of the case, and the statute the defendant is suspected of violating. Prior to 2015, any case involving a suspected felony received a retention code of zero, indicating that all evidence in the case would be retained indefinitely. When the sheriff's department implemented the PRELIMS system to manage its cases in 2015, this system changed. Although cases continue to be classified with URN's, and the first digit of the URN is still referred to within the sheriff's department as a retention code, this code no longer indicates how long evidence in a case will be retained. Instead, the sole determining factor is the final three digits of the URN, known as the "stat code." The stat code corresponds to the statute the defendant is suspected of violating. In the case of some "wobbler" offenses, which can be prosecuted either as misdemeanors or as felonies (see § 17, subd. (b)), the system classifies the offense as a misdemeanor but may still assign a first-digit retention code of zero.

Deputy Cienfuegos booked Field's laptop and the thumb drive into evidence at the sheriff's station in Lost Hills on August 5, 2016. Deputy Cienfuegos entered information about the case into the computer and indicated that the suspected offense was possession of child pornography. The computer system generated a URN: 016043572241137. Because the first digit was a zero, Deputy Cienfuegos and the other sheriff's deputies investigating Field believed that the case was classified as a felony, and that the sheriff's department would retain the evidence indefinitely. Although section 311.11, subdivision (a) defines possession of child pornography as a felony, the statute allows for punishment as if it were a wobbler: either "by imprisonment in the state prison, or a county jail for up to one year, or by a fine." The "stat code" for possession of child pornography in the PRELIMS system is 137, which the system classifies as a misdemeanor.

Because the computer system treated the case against Field as a misdemeanor, pursuant to sheriff's department policy the computer was transferred to a disposal location for electronic waste and was destroyed on June 8, 2017, approximately 10 months after Deputy Cienfuegos booked it into custody. The USB thumb drive was destroyed shortly afterward. None of the sheriff's deputies involved in the case received a warning that the evidence was about to be destroyed.

Howard, the manager of the sheriff's department evidence system, testified that "[t]he software worked exactly as it's

⁷ The sheriff's department policy is to destroy evidence in misdemeanor cases after six months, but the department's software notifies personnel to dispose of evidence only after 10 or 12 months.

Cienfuegos made any mistakes in booking the evidence, because the computer system would have automatically categorized a case involving the violation of section 311.11, subdivision (a) as a misdemeanor. In order to categorize the case as a felony, Deputy Cienfuegos would have needed to enter the charge not as possession of child pornography, but as an unlisted "other felony." Howard suggested that it was the responsibility of the investigating deputy in the case, not the deputy who booked the evidence, to put a hold on the evidence to prevent it from being destroyed. Howard believed it would be a good idea to send a memo to deputies advising them to err on the side of caution and book all cases involving wobbler offenses as felonies.

When he first examined the computer, Detective King was able to make a "mirror image" copy of its hard drive. Sheriff's deputies investigating the case were unable, however, to verify the serial number of the computer to resolve a discrepancy in the sheriff's department file. Nor were they able to power on the computer to check whether its clock was accurate. Because the computer and flash drive had been destroyed, Field and his attorney never had a chance to inspect the computer themselves.

2. Legal Analysis

The United States Supreme Court addressed the question of the state's obligation to preserve evidence in *Trombetta*, *supra*, 467 U.S. 479. The Court held that, at most, the state is required to preserve evidence "expected to play a significant role in the suspect's defense. To meet this standard . . . , evidence must both possess an exculpatory value that was apparent before the evidence was destroyed, and be of such a nature that the defendant would be unable to obtain comparable evidence

by other reasonably available means." (*Id.* at pp. 488–489, fn. omitted.) In *Arizona v. Youngblood* (1988) 488 U.S. 51, 57-58 (*Youngblood*), the Court clarified that "unless a criminal defendant can show bad faith on the part of the police, failure to preserve potentially useful evidence does not constitute a denial of due process of law."

We apply a two-step inquiry to determine whether the failure to preserve evidence violated a defendant's right to due process: "First, did the destroyed evidence meet either the 'exculpatory value that was apparent' or the 'potentially useful' standard for materiality under *Trombetta* or *Youngblood*, respectively? (See *Youngblood*, supra, 488 U.S. at p. 58; *Trombetta*, supra, 467 U.S. at pp. 488–489.) Second, if the evidence qualified as 'potentially useful' under *Youngblood* but did not meet the *Trombetta* standard, was the failure to retain it in bad faith? (*Youngblood*, supra, 488 U.S. at p. 58.)"8 (*People v. Alvarez* (2014) 229 Cal.App.4th 761, 774 (*Alvarez*); see also *City of Los Angeles v. Superior Court* (2002) 29 Cal.4th 1, 11–12.)

In this case, there was no apparent exculpatory value in the computer and the flash drive at the time they were destroyed. Indeed, they appeared to be incriminating, not exculpatory,

⁸ Field argues that this test does not apply in this case because "this does not only concern potentially exculpatory evidence offered to disprove the prosecutor's case, but rather, evidence required to make the prosecutor's case." He cites no law supporting this contention that the ordinary standards of *Trombetta* and *Youngblood* should not apply in his case. To the extent he intends to argue that there was insufficient evidence to support his conviction as a result of the destruction of the computer, we reject that argument. (See Discussion part III, *post.*)

because they connected Field with the charge of possession of child pornography. Nor did the destruction of the computer significantly prejudice Field—because Detective King made a perfect copy of the computer's hard drive, Field was able to access most of the relevant evidence in the case even after the computer was destroyed. The record suggests that the laptop itself could have been useful for only one purpose: 10 its BIOS, or Basic Input Output System, could have been tested to determine whether the computer's clock was accurate. This in turn would have helped establish whether the dates and times recorded in the hard drive image were in fact the times when the child pornography was downloaded and accessed. It is unlikely that this information would have helped with Field's defense, however. The copy of the hard drive indicated that Windows 7 was installed on the computer on March 19, 2016, the same date that Field purchased the computer from Fry's Electronics. This indicates that the computer's clock was accurate as of the time Field purchased the computer. In addition, the child pornography was located in a file directory within the B. Harlan Field user account, which was also created on March 19, 2016. This strongly suggests that the

⁹ The USB flash drive merely contained copies of files from the laptop but did not show the location within the laptop's hard drive, nor when the files were originally downloaded or accessed. The flash drive was therefore of minimal evidentiary value in the case.

¹⁰ In addition, the laptop could have resolved a discrepancy in the serial number sheriff's deputies recorded for the laptop. But that discrepancy appears to have been solely a transcription error. Field did not deny that the laptop the sheriff's deputies seized belonged to him.

pornography was downloaded after Field purchased the computer and created the account.

The lost evidence in this case is thus even less likely to aid the defense than the evidence in Youngblood, where the police failed to preserve a sexual assault victim's clothing so that blood and semen samples on it could be properly tested. (Youngblood, supra, 488 U.S. at p. 54.) The Court held that this evidence was not apparently exculpatory; instead, "no more can be said than that it could have been subjected to tests, the results of which might have exonerated the defendant." (Id. at p. 57.) Because the evidence in this case was at most "'potentially useful'" to the defense (Alvarez, supra, 229 Cal.App.4th at p. 774), Field's right to due process was not violated unless the sheriff's department acted in bad faith by destroying it. The trial court found that the sheriff's department did not act in bad faith, and we must defer to that conclusion if substantial evidence supports it. (See *People* v. Memro (1995) 11 Cal.4th 786, 831, overruled on another ground by *People v. Gaines* (2009) 46 Cal.4th 172, 181, fn. 2.)

The destruction of the evidence in this case is troubling. The testimony of sheriff's deputies paints a picture of a computer system where design flaws created a high degree of risk that evidence would be inadvertently destroyed in a case like this one. The system required a deputy filing a new wobbler case to take extra steps to ensure that evidence would be preserved, while giving no indication that such steps were required. The existence of a retention digit at the beginning of the URN gave deputies a false sense of security that evidence in a case would be retained, making it even less likely that a deputy would realize the mistake. The acknowledgement by the manager of the system that "[t]he software worked exactly as it's intended to"

in this case is alarming and should spur those in charge of the system to action. The proposal to send a memo to deputies countywide warning them of the issue seems inadequate as long as the way the computer system handles wobbler cases is not changed.

Nevertheless, a poorly designed computer system does not constitute bad faith: "The presence or absence of bad faith by the police for purposes of the Due Process Clause must necessarily turn on the police's knowledge of the exculpatory value of the evidence at the time it was lost or destroyed." (Youngblood, supra, 488 U.S. at pp. 56-57, fn. *.) All available evidence indicates that no one working on Field's case within the sheriff's department had any idea that evidence was at risk of being destroyed until it actually happened. There is no indication of "a calculated effort to circumvent the disclosure requirements established by Brady v. Maryland [(1963) 373 U.S. 83] and its progeny," nor any "allegation of official animus towards [the defendant] or of a conscious effort to suppress exculpatory evidence." (Trombetta, supra, 467 U.S. at p. 488; cf. U.S. v. Zaragoza-Moreira (9th Cir. 2015) 780 F.3d 971, 979 [federal agent knew of potential exculpatory value of video surveillance footage and therefore acted in bad faith by failing to preserve it].) The flaws in the sheriff's department computer system seem likely to lead to the destruction of exculpatory and inculpatory evidence equally, favoring neither prosecutors nor defendants. The destruction of the computer and flash drive did not violate Field's right to due process.

C. Sufficiency of the Evidence

Field contends that there was no substantial evidence to support his conviction. He argues that there was insufficient evidence to allow a jury to conclude that he "knowingly possess[ed]" images of child pornography. (§ 311.11, subd. (a).) We disagree.

In reviewing sufficiency of the evidence appeals, we ask "whether, on the entire record, a rational trier of fact could find the defendant guilty beyond a reasonable doubt. . . . [W]e must view the evidence in the light most favorable to the People and must presume in support of the judgment the existence of every fact the trier could reasonably deduce from the evidence." (*People v. Ochoa* (1993) 6 Cal.4th 1199, 1206.)

Field claims to have identified several weaknesses in the prosecution's case. He notes that Detective King, who created the image of Field's hard drive and testified about its contents, could identify only the creation date of folders containing child pornography, but not the images and videos themselves. He also points out that because the laptop was destroyed, investigators could not test the computer to determine whether its system clock was accurate. He also notes that sheriff's deputies did not attempt to determine the prior owner of the computer and investigate whether that prior owner downloaded the child pornography.

But none of these alleged weaknesses casts doubt on the sufficiency of the evidence. Detective King testified that the hard drive image indicated that Windows 7 and the B. Harlan Field user profile were created on March 19, 2016, the same date Field purchased the computer. A reasonable jury could have concluded that the computer's clock was working properly at that

time, and that the creation dates of the folders containing child pornography were likewise accurate. In addition, Detective King testified that the creation dates of ".lnk" shortcut files on the computer indicated that the files themselves had been accessed, even if the creation date was available only for the folders containing the files. Finally, the hard drive image showed that all the child pornography on the computer was downloaded no earlier than June 2016, months after Field bought the computer from Fry's Electronics.

A person can knowingly possess or control child pornography "by actively downloading and saving it to his or her computer." (*Tecklenburg v. Appellate Division* (2009) 169 Cal.App.4th 1402, 1419, fn. 16.) The evidence in this case was sufficient to allow a reasonable jury to find that Field knowingly possessed the child pornography, and that its presence on his computer was not merely inadvertent.

DISPOSITION

The judgment of the trial court is affirmed. $\underline{\text{NOT TO BE PUBLISHED}}$.

ROTHSCHILD, P. J.

We concur:

CHANEY, J.

BENDIX, J.