

## Pride or Prejudice? Detective Darcy's Undercover Social Media Account

BY RAHUL GUPTA

In the literary classic *Pride and Prejudice* by Jane Austen, there is a famous quote about vanity and pride.

Vanity and pride are different things, though the words are often used synonymously. A person may be proud without being vain. Pride relates more to our opinion of ourselves, vanity to what we would have others think of us.<sup>[1]</sup>

Although written over 100 years ago, with the advent of selfies and social media, the quote is more relevant now than ever. It is only fitting that in the case of *People v. Pride*, the defendant's own vanity in posting an incriminating video to social media was the key evidence that led to his conviction. This case unfolds like a three-act play. So grab some popcorn, silence your phones, and enjoy the show.<sup>2</sup>

### First Act: The Basic Facts

In 2017, on a beautiful May evening in San Diego, our leading man, a young male victim, was strolling along the area near Petco Park looking for a taxi. The victim was from out of town and claimed to have become lost using the trolley system. The victim befriended a group of other young men who were looking for a party. Instead of asking about the nearest taxi stand, the victim inquired about purchasing marijuana. The new-found friends responded by jumping the victim with the defendant yelling out, "This is West Coast!" or "West Coast Crips!"<sup>3</sup> The now unfriendly group proceeded to use force to separate the victim from his belongings. During the fight, the defendant took the victim's gold chain necklace. Although overwhelmed by the group, the victim was able to see a distinctive scar along the defendant's jawline. The victim called 911 and described the robbery suspects to arriving officers as gang members.

The next day, after hearing the description of the robbery, a local gang detective began searching social media for evidence of the crime. The gang detective routinely used several undercover social media accounts to monitor gang activity. The gang detective was very familiar with the West Coast Crip gang—specifically the defendant. The gang detective knew the defendant was the only West Coast Crip gang member with a distinctive scar on his jaw. The gang

detective then found a video on one of the defendant's social media accounts in which the messages and videos are set to disappear after being viewed.<sup>4</sup> The video message was posted just hours after the robbery and showed the defendant wearing a gold chain and proclaiming, "Oh, check out the new chain dog. Ya feel me? Ya feel me? All on this thang."<sup>5</sup> The victim was then shown a photo lineup and made a tentative identification of the defendant. The gang detective then showed the victim a screenshot of only the gold chain from the video posted by the defendant to avoid tainting the photo lineup. The victim identified the gold chain in the video as his.

Upon serving a search warrant on the defendant's residence, the defendant was arrested, and the police recovered evidence appearing to link the defendant to the crime. The police found the victim's debit card, the jacket the defendant was wearing in the video posted to social media, and the victim's gold chain—located in the most fortunate of places, around the defendant's neck. The defendant was charged with robbery and a gang enhancement in violation of Penal Code sections 211 and 186.22(b)(1).<sup>6</sup>

### Second Act: The Jury Trial

At trial, the diligent prosecutor filed a written trial brief seeking to introduce the social media video found by the gang detective. The court ruled the video was admissible subject to the proper foundation. However, before the prosecutor could even lay any foundation, the defense objected to the video just prior to opening statements.

The defense objected to the video based upon both constitutional and statutory grounds. First, the defense argued his client had an expectation of privacy in the video because the social media platform allowed private messages to be sent to selected friends and not the general public. Additionally, the defendant's expectation of privacy was heightened because the messages disappeared after they had been viewed by the intended recipients. Second, the defense claimed the manner in which the gang detective

*continued on page 10*

recovered the video violated the California Electronic Communications Privacy Act<sup>7</sup> (CalECPA) and sought to suppress the video under Penal Code section 1546.4.

In an Evidence Code section 402 hearing, the gang detective testified that he did not log into or hack the defendant's social media account to obtain the video, but created an undercover social media account in which the defendant had accepted the gang detective as a "friend." Therefore, to view the video posted by the defendant, the gang detective was simply logging into his own undercover account and viewing a video message sent from the defendant's social media account. The gang detective readily acknowledged that the defendant did not send the video to the undercover account knowing it was created by a detective. The trial court held there was "no authority for the proposition that false friends are not friends for ... a Fourth Amendment violation."<sup>8</sup> The defense objections were overruled, and the video was played for the jury.

Interestingly, in a separate section 1040 hearing, the gang detective also testified that he had been monitoring the defendant's gang for over three years and used the undercover social media account for investigative purposes. After going in camera, the court ruled there was a privilege and the defense was prohibited from inquiring about the name on the undercover account, the names of any other friends associated with the undercover account, and any URLs or phone numbers associated with the account. However, the defense was allowed to illicit from the gang detective that he obtained access to the video by using a false name to create the social media account. Although the defense did not challenge this issue further, it is interesting to see that the trial court had no problem extending traditional concepts of privilege to modern day surveillance techniques, such as an undercover social media account.

The defendant was then convicted for robbery with the gang enhancement in violation of Penal Code sections 211 and 186.22(b)(1). The defendant subsequently appealed.

### Third Act: The Appeal

On appeal, the defendant raised similar constitutional and statutory objections to the admission of the video the gang detective obtained using the undercover social media account.

In relation to the defendant's challenge under the Fourth Amendment, the court focused its analysis on the defendant's expectation of privacy in messages to "friends" on social media. The court easily held there was no Fourth Amendment violation because the defendant assumed

the risk that one of his social media "friends" may be an undercover officer or that any friend might save the messages and then share them with law enforcement.

"[T]he Fourth Amendment does not guard against the risk that the person from whom one accepts a 'friend request' and to whom one voluntarily disclosed such information might turn out to be an undercover officer or a 'false friend' ... thus, one does not have a reasonable expectation of privacy in incriminating information shared with them."<sup>9</sup>

The court analogized the social media video in this case to *People v. Phillips*, an established California case that does not recognize an expectation of privacy when one party to a phone call discloses the conversation to the police.<sup>10</sup> "There is simply no constitutional principle that prohibits the recipient of a confidence from breaching the trust reposed in him not to disclose it to others, including the police."<sup>11</sup> Interestingly, the court also found that the defendant's specific choice of a social media platform (where messages to his friends disappear once they have read them) did not raise the defendant's expectation of privacy to constitute a violation of the Fourth Amendment.

Although the defendant also challenged the admission of the video under the recently enacted CalECPA, there was not an extensive analysis of section 1546 because the court held CalECPA had no application in this case. CalECPA generally restricts government entities from compelling access to electronic devices or producing electronic communication information without a warrant. However, the court noted the warrant exceptions inherent in the statute, specifically, section 1546.1(a)(3) which states: "This section does not prohibit the intended recipient of an electronic communication from voluntarily disclosing electronic communication information concerning that communication to a government entity."

Here, the gang detective never sought to compel access to the defendant's electronic device or information about the device. Instead, the defendant "voluntarily granted access to his social media account by 'friends' ... One such 'friend' to whom he granted access was an undercover profile account for a police detective."<sup>12</sup> Additionally, the court cited another warrant exception under section 1546.1(c)(4) which states: "A government entity may access electronic device information by means of physical interaction or electronic communication with the device ... [w]ith the specific consent of the authorized possessor of the device."

The court appears to interpret the defendant's voluntary posting of his own video to social media and

*continued on page 11*

## No Warrant Needed to Put GPS Tracker on Parolee's Car: A New Decision from the Ninth Circuit

BY MARY K. STRICKLAND

In a case of first impression, the Ninth Circuit recently determined in *United States v. Korte* that law enforcement does not need a warrant to place a GPS tracker on a parolee's car.<sup>1</sup> This recent decision re-affirms law enforcement's ability to carefully monitor parolees in order to protect the community, solve new crimes, and ensure that recently released prisoners remain law abiding.

### The Old-Fashioned Bank Robber

Kyle Korte was a relic of a bygone age. As Judge Owens noted in his opinion, instead of using the Internet to commit crimes or steal identities, Korte stole money "the old-fashioned way," by robbing banks. After being convicted of a bank robbery, he was paroled in the Los Angeles area. As part of his parole, Korte was subject to search and seizure at any time with or without a search warrant or cause. Korte also agreed that he, his residence, and any property under his control would be subject to search.

Shortly after Korte was paroled, a masked robber committed a series of bank robberies, three of which involved the use of a toy gun. Authorities naturally suspected Korte, not only because of his history of robbing banks, but also because he resembled the masked man in the surveillance videos, and a car registered to his address was spotted at the scene of one of the robberies.

The Los Angeles Sheriff's Department (LASD) put a GPS tracking device on Korte's car without his consent and monitored the car's movements for six days. On the seventh day, LASD learned that the FBI had obtained an arrest warrant for Korte. LASD tracked Korte to a nearby bank, where he appeared to be conducting surveillance on his next target. An officer saw Korte open his trunk and put something inside. The officers then arrested Korte, searched his car, and found the toy gun used in the bank robberies in his trunk.

Korte was indicted for one count of attempted bank robbery and three counts of bank robbery. As relevant here,

*continued on page 12*

### HIGH-TECH from page 10

then voluntarily granting access to the undercover officer as providing "specific consent" and thus not triggering any of the warrant requirements of the statute. However, this interpretation may not be apt given the officer testified that he never accessed the defendant's device to view the video.

As the curtains close and the house lights come on, the moral of our story is clear. *Mr. Pride* suffered no *prejudice* from the admission of the video in which he bragged to his friends about his crime on social media. Even when that friend is an undercover police officer. Maybe now, the defendant has learned the difference between pride and vanity.

### ENDNOTES

1. Jane Austen, *Pride and Prejudice* (1813).
2. *People v. Pride* (2019) 31 Cal.App.5th 133.
3. *Id.* at 136.
4. The specific name of the social media platform used by the defendant was not revealed in the appellate opinion.

5. *Pride, supra*, at 139.
6. The defendant was also charged with being a felon in possession of ammunition (Pen. Code § 3035(a)(1)) but was subsequently acquitted by the jury.
7. Pen. Code §§ 1546.1–1546.4.
8. *Pride, supra*, at 139.
9. *Id.* at 139–140, quoting *Everett v. State* (Del. 2018) 186 A.3d 1224, 1236.
10. *People v. Phillips* (1985) 41 Cal.3d 29.
11. *Id.* at 53.
12. *Pride, supra*, at 141–142.

*Rahul Gupta is a senior deputy district attorney in the Orange County District Attorney's Office, whose work centers on major fraud and cybercrime. He is co-chair of CDAA's High-Tech Crimes Committee and was a technical advisor for the 2019 High-Tech Cryptocurrency and Dark Web Symposium.*