The California Legal Update

Remember 9/11/2001: Support Our Troops; Support our Cops; Stand Up For Our Country

Vol. 25 December 30, 2020 No. 14

Robert C. Phillips (858) 395-0302
Deputy District Attorney (Retired) RCPhill101@goldenwest.net

www.legalupdatesonline.com
www.legalupdates.com
www.cacrimenews.com
www.sdsheriff.net/legalupdates

THIS EDITION'S WORDS OF WISDOM:

"*Not in jail; not in a mental hospital; not in a grave. I'd say so far I'm having a very good day*." (Unknown)

IN THIS ISSUE:

ADMINISTRATIVE NOTES:

Geofence Search Warrants: Ever hear of a "*geofence search warrant*" (AKA; *Reverse Location Warrant*)? I had not, at least until recently turned onto the subject by a concerned investigator. A geofence (or "geo-fence") warrant is a search warrant issued by a court allowing law enforcement to search a database to find all active mobile devices within a particular geofence (or geographical) area during a specified period of time. Such warrants are a relatively new (although increasingly popular) investigative technique used by law enforcement in its attempt to identify a specific suspect in a crime (or, more often, series of crimes) under investigation. Geofence warrants are used to obtain information from databases (such as Google's "Sensorvault") where a user's historical geo-location data is stored. Unlike ordinary warrants for electronic records that identify the suspect in advance of the search, geofence warrants essentially work backwards by scooping up the location data from every device that happened to be within a specifically identified geographical area during a specific period of time in the past. The warrants therefore necessarily allow the government to examine the data from a wide range of individuals wholly unconnected to any criminal activity, with law enforcement agents using their own "unbridled" discretion in attempting to pinpoint a specific device or devices that might be connected to the crime under investigation. Geofence warrants have led to privacy and **Fourth Amendment** concerns where innocent passersby have been subjected to unjustified searches of their Google accounts just by being at a particular location near an active crime scene. This is how geofence warrants work: The government's application for a geofence warrant typically involves a three-step protocol to obtain the information. At the first step, Google, in response to a warrant, produces detailed and "anonymized" (i.e., "having had identifying particulars or details removed") location data for devices that reported their location within the geofence (i.e., a specific geographical area) within one or more specific time periods during which a crime or crimes occurred. Upon receiving the requested information, law enforcement agents then review those records and, at their own discretion, narrow them down to a list of devices for which they desire additional information. The last step is Google being required to produce information identifying the Google accounts for the selected devices. In the process, the Google records of many innocent individuals are necessarily subjected to law enforcement scrutiny. There are no reported appellate court decisions on the constitutionality of geofence warrants in either California, the Ninth Circuit, or the U.S. Supreme Court. However, three lower level federal trial courts, all out of the Seventh Circuit (Illinois), have issued memorandum opinions in response to warrant applications. Two of those opinions explain why applications for such a warrant were denied, noting several constitutional infirmities in their use. (See (1) ***In re Search of Info. Stored at Premises Controlled by Google*** (7th Cir. U.S. Dist. Ct., Nor. Dist., East. Div., of Ill., Aug. 24, 2020) 2020 U.S.Dist. LEXIS 152712, and (2) ***In re Search of Info. Stored at Premises Controlled by Google*** (7th Cir. U.S. Dist. Ct., Nor. Dist. of Ill., July 8, 2020) 2020 U.S.Dist. LEXIS 165185.) A third opinion (see ***In re Search***

Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation (7th Cir. U.S. Dist. Ct., Nor. Dist., East. Div., of Ill., Oct. 29, 2020) 2020 U.S. Dist. LEXIS 201248.) *granted* the agents' application for a search warrant, describing how this particular petition (the warrant itself remaining sealed) differs from the two previous denials. In the two denials, the federal district court magistrates rejected the government's applications for geofence warrants, ruling that the Government's attempts to obtain such a warrant violates **Fourth Amendment** constitutional restrictions on "*overbreadth*" as well as the requirement that warrants describe the items to be seized "*with particularity*." In the third search warrant application, however, the federal magistrate granted the Government's request, going to great lengths in discussing how the agents were able to minimize the constitutional issues by limiting their warrant application in the time spans described (from between 15 to 37 minutes, respectively). They also minimized the geographical locations for which Google's data was to be concerned, typically to a specific roadway or commercial parking lot. As described by the magistrate, the agents "narrowly crafted (the time spans and locations) to ensure that location data, with a fair probability, will capture evidence of the crime only." In writing the warrant application in such a manner, the magistrate noted that the agents limited the warrant request in its scope as much as possible, thus minimizing the constitutional issues. I have the full written decisions (plus a news article summarizing the issue) which I will pass onto you upon request. None of these cases, however, are controlling authority on these issues for what we do in California (state or federal). But the Illinois magistrates' reasoning in each case (being the only published decisions on this issue) cannot be ignored, and will likely be considered when your case—if you're using geofence warrants—is challenged in court. So just be forewarned.

CASE LAW:

***Searches of Vehicles for Marijuana*:**
***H&S Code § 11362.1(c) and the Lawful Possession of Marijuana*:**
***Sealed vs. Closed Baggies of Marijuana in a Vehicle*:**

People v. Hall **(Nov. 24, 2020) 57 Cal.App.5th 946**

Rule: The lawful possession of an ounce or less of marijuana in a vehicle does not, by itself, provide the necessary probable cause to search the vehicle. A baggie of marijuana found in a vehicle need not be sealed to be lawful, so long as it is not actually open when observed.

Facts: At about 11:00 p.m. on September 3, 2018, San Francisco P.D. Patrol Officer Steve Colgan and his partner observed defendant Dontaye T. Hall driving a vehicle with a license plate light out. Initiating a traffic stop and contacting defendant, Officer Colgan observed in plain sight in the center console "a clear plastic baggie, inside of which was a green leafy substance" which appeared to be . . . (*are you ready for this*?) . . . *MARIJUANA*! He also saw in the cup holders "an ashtray filled with ashes," "burnt cigar wrappers, commonly used to wrap marijuana," and "a green leafy substance, that appeared to be broken up" in defendant's lap.

Later, in his testimony, Officer Colgan admitted that he did not attempt to smell the cigar wrappers. There was also no testimony about any smoke being observed or odors that might have been emanating from the vehicle or from defendant himself, or that there was any odor of marijuana at all; burnt or unburnt. It was also admitted by Officer Coglan that defendant did not appear to be under the influence of anything. The officer further admitted in testimony that he had no prior knowledge that defendant might be armed and/or dangerous. It was also apparently assumed (there being no evidence presented on this issue) that the observed marijuana was less than an ounce. It was therefore based solely upon the observed baggie of marijuana that the officers decided to search defendant's vehicle for any additional evidence of the crime of "an open container of marijuana." In searching defendant's car, a pistol was discovered in a backpack on the floor on the rear passenger's side. Charged in state court with carrying a loaded firearm in a public place (P.C. § 25850(a)), carrying a concealed firearm in a vehicle, (P.C. § 25400(a)(1)), and the infraction offense of having no license plate lamp (V.C. § 24601), defendant's motion to suppress the firearm as the product of an illegal search was denied by both the preliminary hearing magistrate and (in a P.C. § 995 motion to dismiss) the trial court judge. Defendant therefore pled no contest in a negotiated plea to a single misdemeanor firearm offense (carrying a loaded firearm) with the remaining charges dismissed. Sentenced to three years of probation and six months in county jail, defendant appealed.

Held: The First Appellate District (Div.2) reversed. On appeal, the People argued that the search of defendant's vehicle was lawful under the so-called "automobile exception" to the search warrant requirement, the officers having observed in plain sight an "open container" of marijuana which provided the necessary probable cause to believe that evidence of a crime would be found. The Court disagreed, noting that observation of an ounce or less of marijuana in a container no longer provides probable cause to believe that more might be found in a vehicle. The Court further held that the baggie of marijuana in this case was not "open;" a necessary element of the crime of illegally possessing an ounce or less of marijuana in a vehicle.
(1) *The Automobile Exception to the Search Warrant Requirement*: It has long been considered an exception to the general search warrant requirement that an officer may search a vehicle without a warrant so long as the officer has probable cause to believe the vehicle contains contraband or evidence of a crime. (*Pennsylvania v. Labron* (1996) 518 U.S. 938, 940; *Robey v. Superior Court* (2013) 56 Cal.4th 1218, 1225.) However, enacted as part of Proposition 64 (November 8, 2016)—legalizing the possession and transportation of up to an ounce (28.5 grams) of marijuana (i.e., "cannabis") by persons 21 years of age or older (see H&S Code § 11362.1(a)(1))—is subdivision (c) of H&S Code § 11362.1, which provides, "[c]annabis and cannabis products involved in any way with conduct deemed lawful by this section *are not contraband* nor subject to seizure, and *no conduct deemed lawful by this section shall constitute the basis for* detention, *search*, or arrest." (Italics added.) Based upon this provision, defendant's possession of marijuana in his car, not being illegal (assuming that defendant's baggie was not "open;" see below), does *not* provide the necessary probable cause to search the rest of his vehicle for more marijuana. As has already been decided by the Fourth District Court of Appeal in *People v. Lee* (Oct. 3, 2019) 40 Cal.App.5th 853, at pg. 862: "(T)he presence of a lawful amount of marijuana in a vehicle cannot, by itself, justify an officer's search for *more* marijuana on the theory that if a person has a lawful amount of marijuana, there may be a greater, unlawful amount of marijuana in the person's car. Instead, 'there must be evidence—that is, *additional* evidence beyond the mere possession of a legal amount—that would cause a

reasonable person to believe the defendant has more marijuana.'" (See *California Legal Update*, Vol. 24, #11, Oct. 28, 2019.) In this case, there is no evidence that defendant was doing anything illegal (again, assuming that the baggie he possessed was unopened). Under the specific terms of H&S § 11362.1(c), therefore, defendant's possession of that baggie cannot be used to establish the necessary probable cause to search the rest of his car for more marijuana. (See also *People v. Shumake* (Dec. 16, 2019) 45 Cal.App.5th Supp. 1 [*California Legal Update*, Vol. 25, #5, Aug. 16, 2020)], and *People v. Johnson* (June 15, 2020) 50 Cal.App.5th 620 [*California Legal Update*, Vol. 25 #9, July 14, 2020].)

(2) *An Open Baggie of Marijuana*: The People argued on appeal that defendant's possession of his baggie of marijuana was not lawful because it was open, or at least had been opened at one time, taking it's possession out from under the protection of H&S Code § 11362.1(c). Pursuant to subdivision (a)(4) of section 11362.1, a person is not permitted to "[p]ossess an open container or open package of cannabis or cannabis products while driving, operating, or riding in the passenger seat or compartment of a motor vehicle, boat, vessel, aircraft, or other vehicle used for transportation." Unfortunately, there was no evidence presented during the motion to suppress as to whether defendant's baggie was actually open or not. Either way, however, the superior court magistrate assumed that the baggie was not "*permanently sealed*," and therefore had to be in violation of section 11362.1(a)(4). On appeal, however, the Appellate Court held that the lack of a permanent seal is not relevant to the issue of whether or not a baggie is "*open*," for purposes of section 11362.1(a)(4) and (c). Prior case authority has held, for instance, that a baggie being merely "knotted at the top" is *not* an open container. (*People v. Johnson*, *supra*.) Other authority, state and federal (albeit trial-level court decisions, and both decided after the events leading up to this current decision), has held that section 11362.1(a)(4) does not require that the container of marijuana be sealed in order to be closed. (See *People v. Shumake* (2019) 45 Cal.App.5th Supp. 1 [*California Legal Update*, Vol. 25, #5, Apr. 16, 2020]; and *United States v. Talley* (June 15, 2020) __ F. Supp.3rd __ [2020 U.S. Dist. LEXIS 106004] [*California Legal Update*, Vol. 25, #13, Nov. 29, 2020].) It is the People's burden to prove every element of an offense. Having failed to prove that defendant's baggie was actually open (as opposed to "knotted at the top," or even just zipped shut), the Appellate Court had to assume that it was closed. Further, the Court rejected the People's alternate argument that other apparent loose marijuana observed in defendant's vehicle (ashes in an ashtray and some "green leafy substance that appeared to be broken up" marijuana in defendant's lap) constituted marijuana in an open container. Per the Court: "Nothing in the record indicates the magistrate considered the ash, 'remnants,' and/or the substance on Hall's lap to constitute either an 'open container or open package of cannabis or cannabis products,'" or that what was observed constituted a "usable amount."

Conclusion: Defendant's possession of an ounce or less of marijuana in his vehicle was lawful pursuant to H&S Code § 11362.1(a)(1) and (a)(4). As such, subdivision (c) of section 11362.1 commands that defendant's marijuana is not to be considered contraband nor subject to seizure, nor constitute a legal basis for defendant's detention, search, or arrest. Defendant's conviction, therefore, was reversed. The matter remanded to the trial court with directions to set aside its order denying the motion to suppress, enter an order granting the motion, allow defendant to withdraw his plea, and conduct further proceedings consistent with this opinion.

Note: The burning issue (pardon the pun) left undecided is what it takes, in addition to the lawful possession of marijuana, to give an officer the probable cause he needs to conduct a full

warrantless search of the suspect's vehicle. I believe we can still make the argument with a straight face that if, in the officer's training and experience, he or she "*smells*" what he or she can honestly testify to as indicative of either "bulk" or "burning" marijuana (it still being illegal to possess more than an ounce of marijuana (H&S § 11357) and/or smoke while driving (H&S §§ 11362.3(a)(7)) or riding as a passenger in (H&S § 11362.3(a)(8)) a motor vehicle), then a full vehicle search for the source of that odor is lawful. It might be argued that *People v. Johnson* (2020) 50 Cal.App.5th 620, seems to say otherwise. The Court in *Johnson* held to be *illegal* a search of a vehicle based upon the odor of marijuana and the observation of a small knotted baggie of marijuana in the center console. My counter argument is that if the odor can be accounted for *only* by the legal baggie that is observed, as was apparent in *Johnson,* then we're done. But if not, such as when it smells like "*bulk*" or freshly "*burnt*" marijuana, then we have the necessary probable cause to go looking for the source of that odor. There was no testimony in *Johnson* of the odor of "*burning*," or "*bulk*," marijuana, either of which, had it been observed, would have indicated a violation of H&S Code § 11362.1. Other jurisdictions tend to agree with me. For instance, in Colorado, where recreational marijuana use is also lawful, it has been decided that despite such legalization, "a substantial number of other marijuana-related activities remain unlawful under Colorado law. Given that state of affairs, the odor of marijuana is still suggestive of criminal activity." (*People v. Zuniga* (Colo. 2016) 372 P.3rd 1052, 1059 [2016 CO 52]; see also *Robinson v. State* (Md.Ct.App. 2017) 451 Md. 94 [152 A.3rd 661, 664–665], from the state of Maryland, in support of this same argument.) So make some California or Ninth Circuit case law for me and we'll see how this argument holds up.

***Law Enforcement's Use of a Ruse and the Fourth Amendment*:**
***Lawful vs. Unlawful Ruses*:**

United States v. Ramirez **(9th Cir. Sept. 25, 2020) 976 F.3rd 946**

Rule: A law enforcement officer may not constitutionally use a ruse that involves misrepresentations as to his or her authority. A federal officer claiming to be a state law enforcement officer, and luring a suspect back to the scene of the execution of a search warrant under false pretenses, violates the public trust and is a Fourth Amendment violation.

Facts: Investigating the Internet distribution of child pornography, the FBI looked into something called "BitTorrent," described as a file sharing network that is publicly available and which uses peer-to-peer file-sharing, allowing a computer to share and download files from other computers. This led to an Internet protocol ("IP") address at an account registered to defendant Stefan Ramirez's at his home address in Fresno. In checking defendant's IP address, the FBI conducted 23 separate download sessions in November and December 2016, involving over 4,000 still images and 20 videos of suspected child pornography. Conducting a physical surveillance on defendant's home in Fresno, it was noted that a white Chrysler sedan, registered to defendant, was often parked in the driveway. Knowing from experience that computers and other electronic storage devices were commonly stored in one's vehicle, and that someone at that residence—possibly defendant—was "involved in (the) possession, receipt, and/or distribution of child pornography," Special Agent Joshua Ratzlaff obtained a search warrant for the residence along with any "[v]ehicles located at or near the premises that fall under the dominion and control of (defendant) or any other occupant of the premises." Defendant himself was not

specifically named as a person to be searched because although the identified Internet account was in defendant's name, several people were known to live there and it was not yet known for sure who at the residence might be receiving the child pornography. The plan was to speak with defendant when the search warrant was executed in order to verify that he was in fact the person trafficking in child pornography. However, on the day and at the time the warrant was executed (sometime during the spring of 2017), defendant had already left for work. In fact no one was home and the Chrysler was gone when the agents arrived. So instead of beginning the search as authorized by the warrant, Agent Ratzlaff decided to concoct a ruse to lure defendant home by calling him at his work, claiming to be a Fresno P.D. police officer investigating a burglary at the residence and telling him he needed to return home to confirm what was taken. However, on a day when nothing seemed to be going according to plan, defendant did not answer his phone when called. So Agent Ratzlaff called another person believed to also live there, only to find out that that person had moved out some three weeks earlier. At Agent Ratzlaff's request, that person called defendant, leaving him a message. That person then called defendant's mother, who owned the house. Defendant's mother came to the residence and confronted the FBI agents, unlocking the door and letting them inside. At the agents' request, she then called defendant and—continuing the ruse that the police were there and that the house had been burglarized—asked him to come home. Defendant promptly responded, returning the missed call from the FBI while on the way. Agent Ratzlaff reiterated the story that he was a police officer, that there had been a burglary at his home, but they should wait until he arrived home to discuss the matter further. Buying the ruse hook, line and sinker, defendant arrived home in his Chrysler to find armed agents wearing "Police" jackets and full body armor with a staged Fresno police car parked in front of the house. It wasn't until defendant parked his car and approached the agents that Agent Ratzlaff finally revealed his true identity and the real purpose of their investigation, explaining that he had used the ruse to induce him to come home and to speak to him about the FBI's child pornography investigation. Defendant was then patted down for weapons and his phone, wallet, and keys were seized. He was taken into a bedroom where, after being told he was not under arrest but never told he could leave, he was subjected to a 45-minute interview during which he cop'd to knowingly possessing child pornography on his computer. His possessions were not returned until the interview was over. While being interviewed, other agents searched defendant's Chrysler and recovered two laptops and two hard drives, presumably containing child pornography. Charged in federal court with child pornography-related offenses, defendant's motion to suppress was denied. Pleading guilty to one count of the distribution of child pornography in violation of 18 U.S.C. § 2252(a)(2) and sentenced to 12½ years in prison and five years of supervised release, defendant appealed.

Held: The Ninth Circuit Court of Appeal, in a split (2-to-1) decision, reversed, ruling that defendant's motion to suppress should have been granted. The issue on appeal—as it was in the trial court—was whether the ruse used in this case, under these unique circumstances, violated the Fourth Amendment. The trial court ruled that it *did not*; the majority of the Appellate Court ruled that *it did*. The existence in this case of a valid search warrant, authorizing the search of defendant's residence and any vehicle at or near the scene, is undisputed. It is also undisputed that the eventual execution of the warrant, after defendant—responding to the ruse—returned home, was in compliance with the terms of the warrant. Recognizing that "(a)n otherwise lawful seizure can violate the Fourth Amendment if it is executed in an unreasonable manner," the issue here was whether the Agent Ratzlaff's use of a ruse under these circumstances was

unreasonable. While the use of "deceit" (i.e., a "ruse") is lawful under the right circumstances, "not every ruse is reasonable under the Fourth Amendment." In determining whether the use of a ruse is lawful, a court "must assess the reasonableness of law enforcement's use of deception by 'balanc[ing] the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion.'" In attempting to find this illusive line between a lawful and an unlawful ruse, some examples are helpful. It is commonly held that acting undercover, hiding that fact that the undercover agent is a law enforcement officer, is generally legal. (*Hoffa v. United States* (1966) 385 U.S. 293.) But should a law enforcement officer identify himself as such, and then betray the target's trust by claiming to have some legal authority that the officer does not in fact have, such a ruse is *not* lawful (e.g., claiming to have a search warrant when you do not: *Bumper v. North Carolina* (1968) 391 U.S. 543, 548-549.) As noted by the Court: "When a government agent presents himself to a private individual, and seeks that individual's cooperation based on his status as a government agent, the individual should be able to rely on the agent's representations." "The balance of interests shifts significantly (in the defendant's favor) when the government's chosen ruse invokes the public's trust in law enforcement because of the concern that 'people "should be able to rely on [the] representations" of government officials.'" (*United States v. Alverez-Tejeda* (9th Cir. 2007) 491 F.3rd 1013, 1017.) Here, Agent Ratzlaff had a search warrant that included the authority to search any vehicles at or near the targeted residence. This would have included defendant's Chrysler had it been there at the time. Agent Ratzlaff also hoped to talk with defendant and obtain admissions to his involvement in the alleged crimes (as he eventually did). The U.S. Supreme Court has established a rule that a law enforcement officer, upon contacting a suspect at the scene of an executed search warrant, has the authority to detain that suspect (and at least attempt to question him) during the execution of the warrant (see *Michigan v. Summers* (1981) 452 U.S. 692; and *Bailey v. United States* (2013) 568 U.S. 186.); referred to here as the "*Summers Rule*." The Court ruled that defendant was in fact detained at the point when he was patted down for weapons and then taken into a bedroom for questioning. But in this case, with neither defendant nor his car before use of the ruse being at the scene where the search warrant was to be executed, both were off limits to detention or search, leaving Agent Ratzlaff with a bit of a dilemma. The Court here found that Agent Ratzlaff's misrepresentations as to his true identity and why defendant was needed back at his home, both made while pretending to be a local police officer and done for the admitted purpose of bringing the Chrysler back to where it could be searched under the authority of the search warrant and to make the "*Summers Rule*" applicable to the situation (allowing for defendant's detention), converted Agent Ratzlaff's misrepresentations into an unlawful ruse. Employing these misrepresentations violated the Fourth Amendment. The Court further found that not only is the evidence recovered from defendant's vehicle subject to suppression, but also his incriminatory statements as well, they being the product of his detention which itself would not have occurred but for the use of the unlawful ruse.

Note: I started reading this case with the preconception (aka; "gut feeling") that overruling defendant's conviction was simply wrong; i.e., that the simple ruse of tricking the defendant into returning home earlier than he otherwise might have planned is not that big a deal; certainly not one of constitutional dimension. And while I've never been comfortable with cops using ruses (believing that to one degree or another, they *all* violate the public's expectation that cops should be honest in all their official acts), they are generally held to be legal, at least so long as it

doesn't result in some false or misleading evidence or perhaps bypass the need for a valid warrant. But aside from that, I still have to question the Court's decision here in that Agent Ratzlaff never misrepresented his authority as a federal agent; an overt action the Court so heavily condemns even though not an issue in this case. All he did was claim to be a different type of law enforcement officer. But on the plus side is the fact that this case—right or wrong—makes for a simple, easy to follow rule: As a law enforcement officer, you cannot make misrepresentations that violate the trust we like to think people have (or should have) in law enforcement, and which as a result subjects someone to a search, detention, or arrest from which that person would have otherwise been constitutionally protected. In this case, defendant would not have been subject to a *Summers*-authorized detention, nor his car subject to search, unless and until they (he and his Chrysler) were present at his house. Looking to the dissenting opinion for some validation of my concerns with this case, I found it to be really more of an emotional appeal, noting that "we are talking in this case about the attempted rape of a two- or three-year-old child. We are talking about tying up a nine-year-old and having a dog do things to her. We are talking about things that are just, beyond description, horrid." While you cannot disagree with the disgusting and disturbing nature of child pornography and the industry that produces it, emotional responses don't address the legalities of the applicable search and seizure law in such cases. The dissent did express a problem in finding a ruse to be illegal where the FBI did no more than execute a search and a detention that was expressly contemplated for by the search warrant and the concurrent "*Summers Rule*," the ruse itself merely speeding up the process by eliminating the need to wait until defendant returned home under his own volition. I think that's my problem with this case as well. But at least—until contrary authority comes down—we know now where to draw the line.

***The Private Search Doctrine*:**
***Google's Computerized hashing technology*:**
***Child Pornography and the Internet*:**

People v. Wilson **(Oct. 21, 2020) 56 Cal.App.5th 128**

Rule: So long as a warrantless search conducted by a government entity is preceded by a private person search, the government search does not implicate the Fourth Amendment as long as it does not exceed the scope of the initial private search. Google, using its proprietary hashing procedures to identify child pornography sent by its subscribers, is a private person search.

Facts: Defendant Luke Noel Wilson, a San Diego resident, liked to use a scam where he would lure young women with acting and modeling aspirations into photoshoots, finding his prospective candidates on a website where the women advertised their availability. Once he got their attention, his plan was to begin the photo sessions with his targets being fully clothed, leading to being partially nude, to totally nude, to "sexually explicit," to overt pornography, sometimes with himself participating. The transition was eased through the use of alcohol and monetary payments. One such connection was an 18-year-old woman who soon introduced defendant to her younger sister; 15-year-old J.A. Defendant gradually led J.A. through the above progression, a relationship that lasted for several years until she was a young adult, and even after she became pregnant via a boyfriend when she was 17. Not yet satisfied, or perhaps just broadening his repertoire of pornographic photographs, defendant eventually coxed J.A. into

photographing herself sexually abusing her infant daughter as well as a five-year-old cousin, paying her for the photos. Much of the exchange of photographs was accomplished via the Internet, with defendant using his Google Gmail account. J.A. eventually began to feel guilty about committing acts that she knew were wrong (i.e., abusing her daughter and cousin), telling defendant that she was done even though she continued to sit for photoshoots of herself for him. But then she got busted by the F.B.I. and charged with felony child abuse (per P.C. § 273a(a)), and, under a plea bargain, was sentenced to 10 years of probation. Meanwhile, Google became aware that defendant was transmitting child pornography via his e-mail Gmail account. Google uses a screening process that employs a "proprietary 'hashing' technology" to identify apparent child sexual abuse images on its services. This is how it works: (This is all Greek to me, so I pretty much plagiarized this from the Court's decision itself.) Since 2008, Google has used a computerized "hashing technology" to assist in this process. It starts with trained Google employees using software to generate a "hash" value for any image file they find depicting child pornography. At least one Google employee reviews some random offending child pornography image before it is assigned a unique hash value, or a "digital fingerprint," that is then stored in Google's repository of hash values. This hash value is generated by a computer algorithm and consists of a short alphanumeric sequence that is considered unique to the computer file. The resulting hash values are then added to a repository. The repository therefore contains hash values, not the actual child pornography images. When a user uploads new content to its services, Google automatically scans and generates hash values for the uploaded files and compares those hash values to all known hash values in the repository. If Google's system detects a match between a hash value for uploaded content and a hash value in the repository for a file which was previously identified as containing apparent child pornography, the system generates a report to be sent to the National Center for Missing and Exploited Children (NCMEC) in the form of a "Cybertip" NCMEC is statutorily obligated to serve as a national clearinghouse and maintain a tip line for Internet service providers to report suspected child sexual exploitation violations. (18 U.S.C. § 2258A(c)) Also by statute, NCMEC is obligated to forward those reports to federal law enforcement. It may also (as it did in this case) forward the reports to state and local law enforcement. In the process, Google may or may not open the image file for manual review to confirm it contains apparent child pornography. In June, 2015, Google's system identified four image files, each with hash values matching values for apparent child pornography images in its repository, attached to an e-mail created by a Gmail account later identified as belonging to defendant. Google generated a Cybertip report to NCMEC identifying and forwarding the four image attachments. The report included only the four image files, not the e-mail body text or any other information specific to the e-mail. Google classified the images, using a common categorization matrix, as "A1," indicating they depicted prepubescent minors engaged in sex acts. The report reflected that a Google employee did not manually review these specific files after they were flagged using Google's hashing technology, and before sending them to NCMEC. Upon determining that the Gmail account at issue was in San Diego, NCMEC forwarded it onto the "San Diego Internet Crimes Against Children" (ICAC) task force. This task force is comprised of law enforcement individuals from multiple agencies, including the San Diego Police Department (SDPD). When the ICAC received the report, an administrative assistant with SDPD printed the report with the attached electronic images and provided them to two ICAC investigators. These investigators opened the files, viewed the images, and determined that the images warranted an investigation. An ICAC sergeant conducted his own review and agreed with that recommendation. Using the information

contained in the report and based on his own review of the images, ICAC Investigator William Thompson obtained a search warrant requiring Google to provide all content and user information associated with the identified Gmail address. The warrant resulted in the discovery of defendant's e-mails offering to pay J.A. to molest and exploit children. Thompson also reviewed e-mails in which defendant distributed child pornography to others. This led to another search warrant authorizing the search of defendant's apartment and vehicle, the execution of which resulted in the seizure of computer equipment, storage devices, and other effects as well as a thumb drive containing thousands of images of child pornography. Additional images were found on devices in defendant's apartment. Charged in state court with a whole pile of child pornography-related offenses, defendant filed a motion to suppress which the trial court denied. He therefore went to trial, the jury convicting him on all counts. Sentenced to an indeterminate term of 45-years-to-life, defendant appealed.

Held: The Fourth District Court of Appeal (Div. 1) affirmed defendant's conviction. Among the many issues decided on appeal was the lawfulness of the search of defendant's thumb drive and computers, etc., defendant arguing that it was all the product of an illegal warrantless search of his e-mail account conducted by Google, with law enforcement using that allegedly illegally seized information as a basis for the warrants obtained by ICAC Investigator Thompson. Defendant also argued that when Investigator Thompson initially looked at his (defendant's) photographs without a search warrant, he did so illegally. At defendant's motion to suppress, Thompson testified about his investigation, acknowledging that neither Google nor NCMEC had opened the image files attached to defendant's e-mail, and that he himself did not obtain a search warrant before first viewing the attachments. The general rule is that searches and seizures are presumed to be illegal; i.e., in violation of the Fourth Amendment, absent a search warrant or some other legally recognized exception. "Private searches" (i.e., searches conducted by private persons) are exempt from this rule. The suppression requirements of the Fourth Amendment do not apply to searches by private persons. Taking it a step further, the United State Supreme Court has held that "if a government search is preceded by a private search, the government search (also) does not implicate the Fourth Amendment *as long as it does not exceed the scope of the initial private search*." (Italics added; *United States v. Jacobsen* (1984) 466 U.S. 109, 115–117.) In other words, so long as law enforcement, in making a warrantless search, does not view anything a private person or entity hasn't already seen, the Fourth Amendment is not implicated. Typically, this involves some private party opening a container and viewing contraband, and then notifying law enforcement of his or her discovery with law enforcement then repeating what the private person has already done. *Jacobson* covers this type of situation, saying that this is all legal, having been initiated by a "private person search." In this case, the Court held that Google's actions of scanning user content, assigning hash values to that content, comparing user content to a repository of hash values, flagging offending images with hash values that match previously reviewed child pornography images, and then sending the apparent child pornography to NCMEC, is substantially the same, constituting in effect private action that was not performed at the direction of the government. Therefore, Investigator Thompson in this case did not violate the Fourth Amendment when he opened and viewed the four photographs that Google (as, in effect, a private person) had flagged as pornography via it's hashing procedure. Thompson having viewed what Google had marked as pornography, and his subsequent search warrants, therefore, were lawful, as was the eventual discovery of the child pornography in defendant's computers and thumb drive being used in evidence against him at trial.

Note: The Court's written analysis is a lot more complicated than my summary, above. And it took me (not being the most brilliant person when it comes to computer technology) several readings to make sense of it all so that I could simplify it enough to get it down to its basics. If you're still confused, just know that when Google sends you ("you" being law enforcement) something that it says its "hashing" system has identified as pornography, you can take a look at what Google sent you without a warrant to see if you agree, and if so, then get your warrants for the identified suspect's computers. That's really all the above legal mumbo jumbo and computer gobbledygook says.