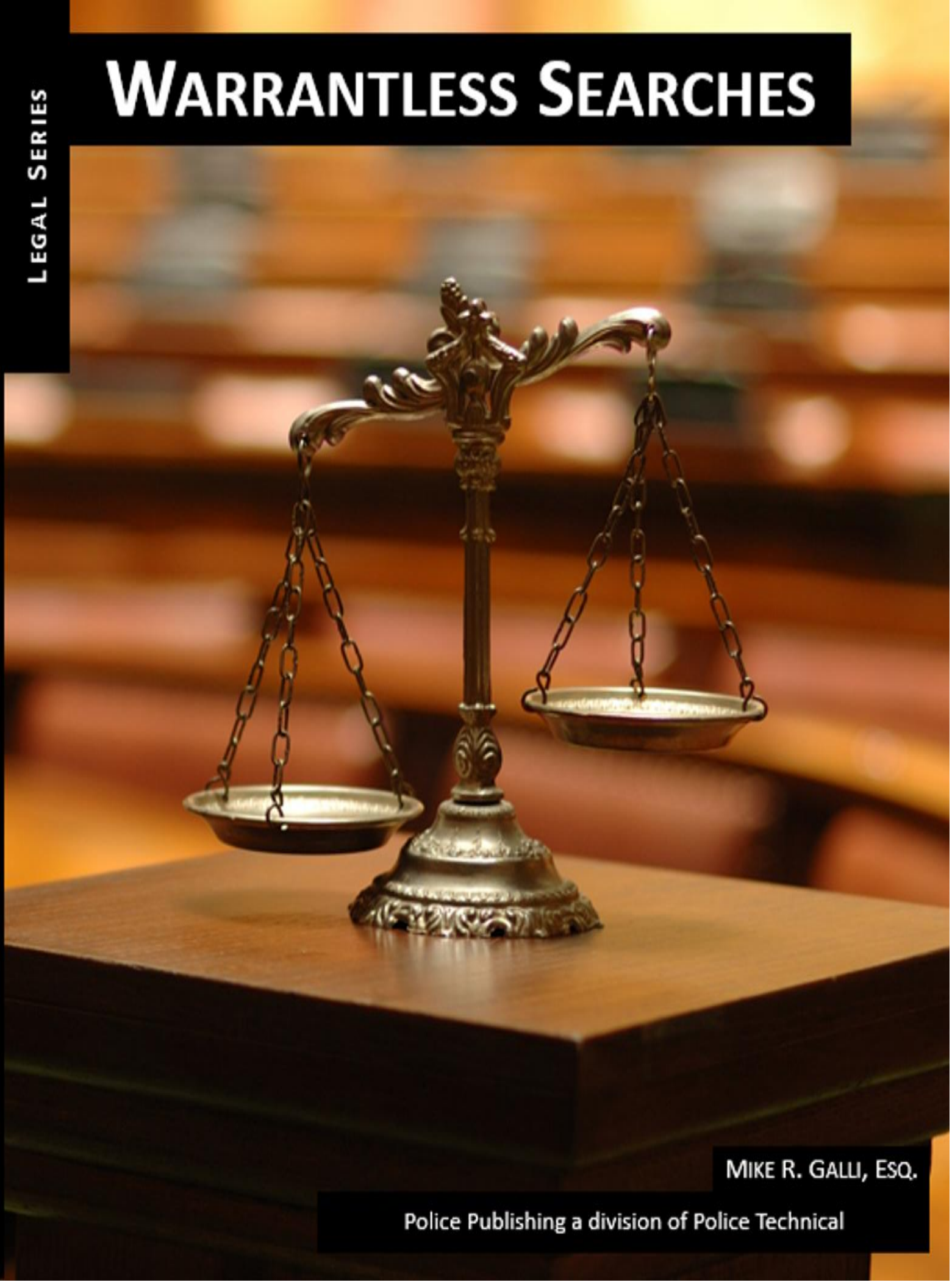
LEGAL SERIES

WARRANTLESS SEARCHES



MIKE R. GALLI, ESQ.

Police Publishing a division of Police Technical

Letter from the Publisher about the EVALUATION COPY

Thank you for downloading this evaluation copy of Warrantless Searches by Mike R. Galli.

The following materials are excerpts (Table of Contents and Chapter 2.4) from the upcoming book, Warrantless Searches by Mike R. Galli, first in the "Legal Series" from POLICE PUBLISHING, a Division of POLICE TECHNICAL.

Warrantless Searches' first edition will be released in January 2015. In development for over a year, Warrentless Searches is nearly 300 pages long with over 350 cited cases. It contains updated material on the recent Supreme Court ruling regarding cell phones. Although, many of the cases discussed in this book are based in California, they are still applicable across the United States.

This evaluation copy is provided to U.S. law enforcement personnel for evaluation and comment.

If you would like to share your comments about this document please contact:

Brianne Hofmann
POLICE PUBLISHING, Editor
bhofmann@policetechnical.com
812-232-4200

Pre-Sale Orders

If you would like to purchase pre-sale copies of Warrantless Searches by Mike R. Galli, please visit POLICETECHNICAL.com. The single distribution price will be set at $105.00; the pre-sale order price is $60.00. Presale orders will be taken until January 2015.

Thank you for reading the following excerpts from Warrantless Searches by Mike R. Galli, and thank you for your interest in POLICE PUBLISHING.

Respectfully,

Thomas M. Manson
POLICE TECHNICAL, CEO
POLICE PUBLISHING, Publisher
tmanson@policetechnical.com

Table of Contents

2.4 – Cell Phones

On June 25, 2014, the U.S. Supreme Court handed down its landmark decision in **Riley v. California** (2014) 573 U.S. ___ ; 134 S.Ct. 2473 (companion case **United States v. Wurie** (2013) 728 F.3d 1), in which it addressed—for the first time—the Fourth Amendment and cell phone searches. The Supreme Court reached the same result in both *Riley* and *Wurie*. Chief Justice John Roberts wrote the Court's opinion, with Justice Alito writing a separate, concurring opinion.

The rule unanimously enunciated by the U.S. Supreme Court is that the police **may not** generally search through digital information on a seized cell phone, incident to a lawful arrest, without first obtaining a search warrant. The holding specifically rejected the rationale put forth by some lower courts that allowed the search of a cell phone, incident to a lawful arrest. In reaching its decision, the Court decided that one's privacy interests in the material stored on a cell phone outweighed any justification put forth by the United States and California governments in support of a warrantless search exception.

The Court noted in the context of privacy issues how unique cell phones are in the digital age compared to other physical items people normally carry on their person:

> The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months as would routinely be kept on a phone.
>
> Finally, there is an element of pervasiveness that characterizes cell phones but not physical records. Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception. According to one poll, nearly three-quarters of smart phone[1] users report being within five

[1] **Riley**, **supra**, at 2480. The Court defined a "smart phone" as "a cell phone with a broad range of other functions based on advanced computing capability, large storage capacity, and Internet connectivity."

> feet of their phones most of the time, with 12% admitting that they even use their phones in the shower. [Citation.] . . .Today, by contrast, it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate. [Citation.] Allowing the police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case.
>
> Although the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different. An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD. Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building. [Citation.] . . . ¶ Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.

(**Riley**, **supra**, at 2489–2491.)

Chief Justice Roberts acknowledged the impact the Court's ruling would have on law enforcement, but explained why the rule announced was necessary:

> We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime. Cell phones have become important tools in facilitating coordination and communication among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals. Privacy comes at a cost.
>
> Our holding, of course, is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest.

(**Id**. at 2493.)

In his concurring opinion, Justice Alito emphasized that he was not convinced that the search incident to arrest doctrine was based exclusively or primarily on the need to protect the arresting officer's safety and the need to prevent the destruction of evidence. He also said that while he agreed with the Court's decision, he would reconsider the issue if either Congress or state legislatures enacted legislation that drew reasonable distinctions based on categories of information or other variables. He cited

the example of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 passed by Congress, in response to the Court's decision in **Katz v. United States** (1967) 389 U.S. 347, holding that electronic surveillance constituted a search even when no property interest was invaded.

FACTS (Riley v. California (2014) 573 U.S. ___; 134 S.Ct. 2473 [companion case United States v. Wurie (2013) 728 F.3d])

A police officer stopped David Riley for driving with expired registration tags. In the course of the stop, the officer learned that Mr. Riley's license had been suspended. Accordingly, the officer impounded Mr. Riley's car pursuant to departmental policy. The officer conducted an inventory search of the car. During that search, the officer found two loaded handguns concealed under the car's hood.

Mr. Riley's person was searched incident to arrest and the officer found evidence associating him with the "Bloods" street gang. The officer also seized a "smart" cell phone from Mr. Riley's pants pocket. The officer accessed information on the phone and saw that the letters "CK" preceded some words—a label the officer believed stood for "Crip Killers," as well as a slang term for members of the Bloods gang.

At the police station, approximately two hours after Mr. Riley's arrest, a detective specializing in gangs conducted a further examination of the phone's contents. The detective testified at the suppression hearing that he "went through" the phone "looking for evidence, because . . . gang members will often video themselves with guns or take pictures of themselves with the guns." (*Riley, supra,* at 2480–2481.) Although there were a lot of things on the cell phone, the detective's attention was attracted to particular files including videos of young men sparring while someone yelled encouragement using the moniker "Blood." On the phone, officers found photographs of Mr. Riley standing in front of a car that they suspected had been involved in a shooting a few weeks earlier.

Mr. Riley was ultimately charged—in connection with that earlier shooting—with firing at an occupied vehicle, assault with a semiautomatic firearm, and attempted murder. The charging document also alleged that those crimes had been committed for the benefit of a criminal street gang, which is an aggravating factor under California law and carries an enhanced sentence.

Mr. Riley asked the trial court to suppress all the evidence obtained from his cell phone, arguing that the search of the cell phone violated his Fourth Amendment rights because the search had been conducted without a warrant and was not otherwise justified by exigent circumstances. The trial court rejected Mr. Riley's argument and denied his motion to suppress the evidence. At his trial, officers testified about the photographs and videos found on the cell phone, with some of the photographs even being admitted into evidence. A jury convicted Mr. Riley on all counts, and the court sentenced him to an enhanced sentence of 15 years to life.

Mr. Riley appealed that verdict to the California Court of Appeal, which affirmed the case relying on the California Supreme Court's decision in **People v. Diaz** (2011) 51

Cal.4th 84. The California Supreme Court denied Mr. Riley's petition for review, but the U.S. Supreme Court granted certiorari.

In the **Wurie** case, officers were performing routine surveillance when they saw Brima Wurie make an apparent drug sale from a car. Mr. Wurie was arrested and taken to the police station. At the station, officers seized two cell phones from his person. The cell phone that formed the basis of the appeal was a "flip phone."[2]

Approximately five to ten minutes after arriving at the station, the officers noticed that the phone was repeatedly receiving calls from a source identified as "my house" on the phone's external screen. A few minutes later, the officers opened the phone and saw a photograph of a woman and a baby set as the phone's wallpaper. The officers pressed one button on the phone to access the call log, then another button to determine the phone number associated with the "my house" label. The officers then used an online phone directory to trace that phone number to an apartment building.

When the officers went to the apartment building, they saw Mr. Wurie's name on a mailbox and observed a woman, through a window, who resembled the woman in the photograph on Mr. Wurie's phone. The officers secured the apartment and obtained a search warrant. During the service of the search warrant, the officers seized 215 grams of crack cocaine (approximately 7.5 ounces), marijuana, drug paraphernalia, a firearm and ammunition, and a sum of cash. Mr. Wurie was charged with distributing crack cocaine, possessing crack cocaine with the intent to distribute it, and being a felon in possession of a firearm and ammunition. Mr. Wurie moved to suppress the evidence in the district court, but the court denied his motion. At trial, a jury convicted Mr. Wurie of all three counts and the court sentenced him to 262 months (approximately 21 years and 9 months) in federal prison.

A divided panel of the First Circuit Court of Appeal reversed the denial of the suppression motion. The First Circuit ruled that "cell phones are distinct from other physical possessions that may be searched incident to arrest without a warrant, because of the amount of personal data cell phones contain and the negligible threat they pose to law enforcement interests." (**Riley**, **supra**, at 2482, citing **Wurie**, **supra**, at 8–11.) The United States appealed and the Supreme Court granted certiorari.

RATIONALE

In reaching its decision that the search was unlawful in both cases, the Court relied on three precedents: **Chimel v. California** (1969) 395 U.S. 752; **United States v.**

[2] **Id**. at 2481. The Court defined a flip phone as "a kind of phone that is flipped open for use and that generally has a smaller range of features than a smart phone."

Robinson (1973) 414 U.S. 218; and **Arizona v. Gant** (2009) 556 U.S. 332.[3] Chief Justice Roberts observed:

> When an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or affect his escape. Otherwise, the officer's safety might well be endangered, and the arrest itself frustrated. In addition, it is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction . . .

(**Riley**, **supra**, at 2483, quoting **Chimel**, **supra**, at 762–763.)

In **Robinson**, the Supreme Court applied the **Chimel** analysis in the context of the search of an arrestee's person. The court concluded in that case that the search of Mr. Robinson was reasonable even though there was no concern about the loss of evidence, and the arresting officer had no specific concern that Mr. Robinson might be armed.

Chief Justice Roberts observed that the search incident to arrest doctrine now required the Court to apply that doctrine to modern cell phones, which he observed were "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." (*Riley*, *supra*, at 2484.)

Chief Justice Roberts observed,

> Absent more precise guidance from the founding era, we generally determine whether to exempt a given type of search from the warrant requirement "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." **Wyoming v. Houghton** (1999) 526 U.S. 295, 300.
>
> While **Robinson's** categorical rule strikes the appropriate balance in the context of physical objects, neither of its rationales has much force with respect to digital content on cell phones.

(**Riley**, **supra**, at 2484.)

[3] In a 5–4 decision in **Arizona v. Gant** (2009) 556 U.S. 332, whose facts are similar to those in **New York v. Belton** (1981) 453 U.S. 454, the U.S. Supreme Court modified its earlier holding in **Belton** in two significant ways: First, it ruled that "**Belton** does not authorize a vehicle search incident to a recent occupant's arrest after the arrestee has been secured and cannot access the interior of the vehicle." **Gant**, **supra**, at 355. By comparison, when the arrestee is unsecured and within reaching distance of a car's passenger compartment, such a search is allowed under the twin rationales of **Chimel v. California** (1969) 395 U.S. 752. In so ruling, the Court effectively ended law enforcement's common practice of automatically searching the passenger compartment of a vehicle incident to an occupant's lawful custodial arrest. Second, it held that "circumstances unique to the automobile context justify a search incident to arrest when it *is reasonable to believe that evidence of the offense of arrest might be found in the vehicle*." **Gant**, **supra**, at 335 [italics added].

While the two risks identified in **Chimel** are present in all custodial arrests, there are no comparable risks when the search is of digital data. **Robinson** regarded any privacy interest retained by an individual after arrest as significantly diminished due to the arrest itself. "Cell phones, however, place vast quantities of personal information literally in the hands of individuals. A search of the information on a cell phone bears little resemblance to the type of brief physical search considered in **Robinson**." (**Riley**, **supra**, at 2485.)

The Court therefore declined to extend the **Robinson** rule to cell phone data searches and instead held that officers must generally secure a warrant before they conduct a cell phone search.

Chief Justice Roberts observed,

> Digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape. Law enforcement officers remain free to examine the physical aspects of a phone to ensure that it will not be used as a weapon—say, to determine whether there is a razor blade hidden between the phone and its case. Once an officer has secured a phone and eliminated any potential physical threats, however, data on the phone can endanger no one.

(Riley, **supra**, at 2485.)

In the Court's view, the interest in protecting officers' safety does not justify dispensing with the warrant requirement across the board as it relates to cell phones.

Chief Justice Roberts stated that "once law enforcement officers have secured a cell phone, there is no longer any risk that the arrestee himself will be able to delete incriminating data from the phone." (**Id.** at 2486.)

The Supreme Court rejected the United States and California's argument that information on the cell phone may nevertheless be vulnerable to two types of evidence destruction unique to digital data: remote wiping and data encryption.

> With respect to remote wiping, the Government's primary concern turns on the actions of third parties who are not present at the scene of the arrest. And data encryption is even further afield. There, the government focuses on the ordinary operation of a phone's security features, apart from *any* active attempt by a defendant or his associates to conceal or destroy evidence upon arrest.

(**Id**.)

Chief Justice Roberts noted that the Court had been given little reason to believe that either problem was a prevalent one, and stated:

> [I]n situations in which an arrest might trigger a remote-wipe attempt or an officer discovers an unlocked phone, it is not clear that the ability to

> conduct a warrantless search would make much of a difference. The need to effect the arrest, secure the scene, and tend to other pressing matters means that law enforcement officers may well not be able to turn their attention to a cell phone right away.

(**Id**. at 2487.)

With respect to remote wiping of a cell phone, the Chief Justice pointed out that,

> . . . law enforcement is not without specific means to address the threat. Remote wiping can be fully prevented by disconnecting a phone from the network. There are at least two simple ways to do this: First, law enforcement officers can turn the phone off or remove its battery. Second, if they are concerned about encryption or other potential problems, they can leave a phone powered on and place it in an enclosure that isolates the phone from radio waves.

(**Id**.)

The Court also specifically referred to "Faraday bags":[4]

> If "the police are truly confronted with a 'now or never' situation,"—for example, circumstances suggesting that a defendant's phone will be the target of an imminent remote-wipe attempt—they may be able to rely on exigent circumstances to search the phone immediately. [Citation] Or, if officers happen to seize a phone in an unlocked state, they may be able to disable a phone's automatic-lock feature in order to prevent the phone from locking and encrypting data. [Citation] Such a preventive measure could be analyzed under the principles set forth in our decision in [**Illinois v.**] **McArthur** [(2001)] 531 U.S. 326,[5] which approved officers' reasonable steps to secure a scene to preserve evidence while they awaited a warrant.

(**Riley**, **supra**, at 2487–2488.)

The Court also rejected the United States' argument that a search of all data stored on a cell phone is "materially indistinguishable" from searches of physical items. Chief Justice Roberts responded to the argument by noting that the argument was

> . . . like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together. Modern cell phones, as a

[4] **Riley**, **supra**, at 2487. The Court described Faraday bags as "essentially sandwich bags made of aluminum foil: cheap, lightweight, and easy to use."

[5] In an 8–1 opinion by the U.S. Supreme Court in **Illinois v. McArthur** (2001) 531 U.S. 326, with only Justice Stevens dissenting, the Court ruled that it was reasonable for the police to prohibit the defendant from re-entering his trailer without the police accompanying him, while a search warrant was being sought for the trailer. The Supreme Court ruled that the Fourth Amendment did not prohibit the type of seizure done by the police in this case. Rather than adopting a per se rule of unreasonableness, the court balanced the privacy-related interests of the individual and the law enforcement-related interests to determine if the intrusion was unreasonable.

> category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse. A conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom.

(**Id**. at 2488–2489.)

> Cell phones differ in both a quantitative and qualitative sense from other objects that might be kept on an arrestee's person. The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.
>
> One of the most notable distinguishing features of modern cell phones is their immense storage capacity. Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy. [Citation]
>
> But the possible intrusion on privacy is not physically limited in the same way when it comes to cell phones. The current top-selling smart phone has a standard capacity of 16 gigabytes (and is available with up to 64 gigabytes). Sixteen gigabytes translates to millions of pages of text, thousands of pictures, or hundreds of videos. … [Citation] Even the most basic phones that sell for less than $20 might hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on. [Citation] We expect that the gulf between physical practicability and digital capacity will only continue to widen in the future.

(**Id**. at 2489.)

> To further complicate the scope of the privacy interests at stake, the data a user views on many modern cell phones may not in fact be stored on the device itself. Treating a cell phone as a container whose contents may be searched incident to an arrest is a bit strained as an initial matter. … [Citation] Cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself. Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference. [Citation] Moreover, the same type of data may be stored locally on the device for one user and in the cloud for another.
>
> The United States concedes that the search incident to arrest exception may not be stretched to cover a search of files accessed remotely—that

> is, a search of files stored in the cloud. [Citation] Such a search would be like finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house. But officers searching a phone's data would not typically know whether the information they are viewing was stored locally at the time of the arrest or has been pulled from the cloud.

(**Id**. at 2491.)

The Court further rejected several fallback positions of the United States and California that would have allowed a warrantless search of a cell phone under certain circumstances. The Court reasoned, "[e]ach of the proposals is flawed and contravenes our general preference to provide clear guidance to law enforcement through categorical rules." (**Id**.)

The first proposal was based on **Arizona v. Gant**, and would allow for a search of a cell phone whenever it is reasonable to believe that the phone contains evidence of the crime for which a suspect has been arrested. An example would be the arrest of a drug dealer who was driving a vehicle at the time of the arrest and was in possession of a cell phone. This proposal—and the reasons for its rejection—will be discussed in more detail in Section 2.4.1, Probable Cause and Vehicle Searches.

The United States also proposed a rule that would restrict the scope of a cell phone search to those areas of the phone where an officer reasonably believes that information relevant to the crime, the arrestee's identity, or officer safety will be discovered.

In rejecting that proposed rule, the Court stated:

> This approach would again impose few meaningful constraints on officers. The proposed categories would sweep in a great deal of information, and officers would not always be able to discern in advance what information would be found where.

(**Id**. at 2492.)

The final proposal put forth by the United States and rejected by the Court was that officers should always be allowed to search a phone's call log. In rejecting this proposal, Chief Justice Roberts observed:

> [C]all logs typically contain more than just phone numbers; they include any identifying information that an individual might add, such as the label "my house" in Wurie's case.

(**Id**. at 2493.)

At oral argument, California suggested a different limiting principle where officers could search cell phone data if they could have obtained the same information from a pre-digital counterpart. In rejecting this approach, the Court stated:

> [T]he fact that a search in the pre-digital era could have turned up a photograph or two in a wallet does not justify a search of thousands of photos in a digital gallery. The fact that someone could have tucked a paper bank statement in a pocket does not justify a search of every bank statement from the last five years. And to make matters worse, such an analogue test would allow law enforcement to search a range of items contained on a phone, even though people would be unlikely to carry such a variety of information in physical form. In Riley's case, for example, it is implausible that he would have strolled around with video tapes, photo albums, and an address book all crammed into his pockets. But because each of those items has a pre-digital analogue, police under California's proposal would be able to search a phone for all of those items—a significant diminution of privacy.
>
> In addition, an analogue test would launch courts on a difficult line-drawing expedition to determine which digital files are comparable to physical records. Is an email equivalent to a letter? Is a voicemail equivalent to a phone message slip? It is not clear how officers could make these kinds of decisions before conducting a search, or how courts would apply the proposed rule after the fact.

(**Id**.)

In a 5-2 decision in the case of **People v. Diaz** (2011) 51 Cal.4th 84, the California Supreme Court affirmed the Court of Appeal decision allowing the admissibility of evidence obtained from a cell phone 90 minutes after the defendant's arrest on drug charges. However, in upholding the admissibility of the evidence derived from a search of the cell phone under the "search incident to arrest" theory, that decision is now in direct conflict with the U.S. Supreme Court's decision in Riley v. California, and therefore, is no longer valid.

Since some California searches of cell phones that occurred before *Riley* will be justified based on the decision in **People v. Diaz**, it is important to know the facts of the case and the California Supreme Court's rationale. Those searches should be upheld by reviewing courts based on the U.S. Supreme Court's decision in **Davis v. United States** (2011) 564 U.S. ___; 131 S.Ct. 2419, which held that when the police conduct a search in objectively reasonable reliance on binding appellate precedent, the exclusionary rule does not apply.

Prior to the Supreme Court's landmark decision in **Riley**, the only valid, legal precedent regarding cell phone searches in California was the California Supreme Court's decision in **People v. Diaz**, which was fully applicable and binding on all California law enforcement officers.

FACTS (People v. Diaz (2011) 51 Cal.4th 84)

> On April 25, 2007, at about 2:50 p.m., senior Ventura County Deputy Sheriff Victor Fazio saw Gregory Diaz participate in an informant-related, controlled purchase of Ecstasy. Mr. Diaz drove the Ecstasy seller to the location of the sale, which then took

place in the backseat of the car Mr. Diaz was driving. Immediately after the sale, Deputy Fazio, who had listened in on the transaction via a wireless transmitter worn by the informant, stopped Mr. Diaz's car and arrested him for being a conspirator in the sale of drugs. Deputy Fazio seized six tabs of Ecstasy in connection with Mr. Diaz's arrest and a small amount of marijuana from Mr. Diaz's pocket. Mr. Diaz also had a cell phone on his person. A detective seized the cell phone from Mr. Diaz and gave it to Deputy Fazio.

Deputy Fazio interviewed Mr. Diaz at the Sheriff's station at 4:18 p.m., but Mr. Diaz denied having any knowledge of the drug transaction. At approximately 4.23 p.m.—after the interview was concluded—Deputy Fazio looked at the cell phone's text message folder and discovered a message that read "6 4 80." Based on his training and experience, Deputy Fazio interpreted the message to mean "six pills of Ecstasy for $80." Deputy Fazio showed the message to Mr. Diaz within minutes of discovering it, and Mr. Diaz then admitted participating in the sale of Ecstasy.

The district attorney charged Mr. Diaz with a violation of Health and Safety Code section 11379(a). Mr. Diaz entered a not guilty plea and moved to suppress the evidence derived from the cell phone text message search. After losing his motion in the trial court, Mr. Diaz changed his plea to guilty of transportation of a controlled substance. Sentence was suspended, and the trial court placed him on probation for three years.

The Court of Appeal affirmed that conviction and held that since the cell phone "was immediately associated with [defendant's] person at the time of his arrest," it was "properly subjected to a delayed warrantless search." (*Id*. at 89.)

The California Supreme Court granted the defendant's petition for review,

> to decide whether the Fourth Amendment to the United States Constitution permits law enforcement officers, approximately 90 minutes after lawfully arresting a suspect and transporting him to a detention facility, to conduct a warrantless search of the text message folder of a cell phone they take from his person after the arrest. (**Id**. at 88.)

RATIONALE

In reaching its decision upholding the search of the text message folder in the cell phone, the Court stated that

> the key question in this case is whether defendant's cell phone was "personal property . . . immediately associated with [his] person" (**Chadwick**, **supra**, 433 U.S. at p. 15)[6] like the cigarette package in

6 **United States v. Chadwick** (1971) 433 U.S. 1, involved a 200-pound, double-locked footlocker that had been removed from a train and placed in a waiting car. Federal agents had probable cause to believe it contained marijuana prior to it being placed in the car. The Supreme Court held that a warrant was required to search the luggage, even though it had been transferred to an automobile.

> **Robinson** and the clothes in **Edwards**.[7] If it was, then the delayed warrantless search was a valid search incident to defendant's lawful custodial arrest. If it was not, then the search, because it was "remote in time [and] place from the arrest," "cannot be justified as incident to that arrest" unless an "exigency exist[ed]." (**Chadwick**, **supra**, at p. 15.)

(**Diaz**, *supra*, at 93.)

The Court then said:

> We hold that the cell phone was "immediately associated with [defendant's] person" (**Chadwick**, *supra*, 433 U.S. at p. 15), and that the warrantless search of the cell phone therefore was valid. As the People explain, the cell phone "was an item [of personal property] on [defendant's] person at the time of his arrest and during the administrative processing at the police station." In this regard, it was like the clothing taken from the defendant in **Edwards** and the cigarette package taken from the defendant's coat pocket in **Robinson**, and it was unlike the footlocker in **Chadwick,** which was separate from the defendants' persons and was merely within the "area" of their "immediate control." (**Chadwick**, **supra**, 433 U.S. at p. 15.) Because the cell phone was immediately associated with defendant's person, Fazio was "entitled to inspect" its contents without a warrant (**Robinson**, **supra**, 414 U.S. at p. 236) at the sheriff's station 90 minutes after defendant's arrest, whether or not an exigency existed.

(*Diaz, supra*, at 94.)

Our Founding Fathers wrote the Fourth Amendment with the intention of preventing a general rummaging search of one's possessions by government authorities. Indeed, the decision in *Arizona v. Gant* reinforces this position by allowing a search of a vehicle only if a recent arrestee can gain access to a weapon, or if there is evidence of a crime that might be in the vehicle for which the person is arrested.

Justice Werdegar correctly observes in her dissent that the majority's holding allows

> police carte blanche, with no showing of exigency, to rummage at leisure through the wealth of personal and business information that can be carried on a mobile phone or handheld computer merely because the device was taken from an arrestee's person. The majority thus sanctions a highly intrusive and unjustified type of search, one meeting neither the warrant requirement nor the reasonableness requirement of the Fourth Amendment to the United States Constitution.

---

7 In **United States v. Edwards** (1974) 415 U.S. 800, the Supreme Court upheld the seizure of Eugene Edwards' clothing 10 hours after his 11:00 p.m. arrest and the subsequent seizure from them of paint chips originating from a Lebanon, Ohio, post office window that he attempted to pry open to break into the post office. The Court ruled that the normal process incident to arrest and custody had not been completed, and the delay in seizing Mr. Edwards' clothing was reasonable since substitute clothing could not be found at the late hour of his arrest.

(**Diaz**, **supra**, at 111.)

In **People v. Macabeo** (2014) ___ Cal.App.4th ___ [2014 Cal. App. LEXIS 793], the Court of Appeal found that while the case was on appeal, the U.S. Supreme Court ruled in **Riley**: Absent an emergency, law enforcement was required to obtain a search warrant before searching through the digital contents of a cell phone incident to arrest. However, the appellate court held that based on the U.S. Supreme Court's ruling in **Davis v. United States** (2011) 564 U.S. ___; 131 S.Ct. 2419, and because **Diaz**, was applicable at the time of the search, the officer's actions in conducting a warrantless search of a seized cell phone, incident to a lawful traffic infraction arrest were done in good faith and therefore, the trial court did **not** err by refusing to exclude 18 images of child pornography found on the cell phone.

Another case that is commonly cited as justifying a cell phone search incident to arrest is **United States v. Finley** (5th Cir. 2007) 477 F.3d 250. But like **Diaz**, this case is no longer of any value after the **Riley** decision. **Finley**. also involved the sale of narcotics in a vehicle, but by someone other than Mr. Finley.

FACTS (United States v. Finley (5th Cir. 2007) 477 F.3d 250)

> On August 19, 2005, Midland Texas Police officers were working with the DEA regarding a controlled purchase of methamphetamine from Mark Brown. Amy Stratton was working as an informant with the police on that date. Under the direction of the Midland Police Department (MPD), Ms. Stratton called Mr. Brown and arranged to purchase $600 worth of methamphetamine. Mr. Brown requested that Ms. Stratton travel to his residence to buy the drugs, but pursuant to MPD instructions, she told Mr. Brown that she was at a truck stop in Midland and that she had no transportation to get to his house. Mr. Brown agreed to meet Ms. Stratton at the truck stop. Mr. Brown asked Jacob Pierce Finley for a ride to the truck stop, which Mr. Finley agreed to do. Mr. Finley drove his white-colored, Southwest Plumbing van to the meeting. Mr. Finley's uncle, who also employed Mr. Finley, owned the Southwest Plumbing Company.
>
> Once at the truck stop, Ms. Stratton approached the van's passenger side where Mr. Brown was sitting, and gave him $600 in pre-recorded MPD bills. Mr. Brown gave Ms. Stratton a cigarette package containing a plastic baggie of methamphetamine. According to the lab, 3.1 grams were located inside the cigarette pack, with 1.4 grams being pure methamphetamine. Neither Mr. Brown nor Mr. Finley ever got out of the van.
>
> Mr. Finley drove away from the truck stop, and MPD officers stopped him three to five miles away and searched the van. During the search, they found MPD-marked bills used in the transaction in a trash can between the driver's and passenger seats. They also found two medicine bottles in the trash can. One bottle had an orange top and contained five small plastic bags, two of which contained methamphetamine. The white-capped bottle had a label with the name "Finley" on it. Inside that bottle was a homemade, glass, smoking pipe with methamphetamine residue in it, and a

small piece of straw commonly used to snort narcotics. Also inside the bottle was a plastic bag containing approximately 1.6 grams of a methamphetamine-cutting agent. Both Mr. Finley and Mr. Brown were arrested. A search of Mr. Finley's person yielded a cell phone in his pocket. The phone belonged to Southwest Plumbing and was issued to Mr. Finley for his work; he was allowed to use the phone for personal purposes as well.

During his interview with the police, Mr. Finley admitted to some past cocaine and methamphetamine use, including using the methamphetamine he received from Mr. Brown three days earlier. He admitted to getting his friends marijuana from Mr. Brown on multiple occasions but denied any involvement in the sale of methamphetamine to Ms. Stratton. An MPD officer handed Mr. Finley's cell phone to Special Agent Cook. The agent looked through the phone and found call records and text messages consistent with narcotics trafficking activity. When confronted with these text messages, Mr. Finley claimed that they referred to sales of marijuana and not methamphetamine.

Both Mr. Finley and Mr. Brown were indicted and charged with one count of possession with intent to distribute methamphetamine. Mr. Brown pled guilty and became a cooperating witness in the prosecution of Mr. Finley. Mr. Finley claimed at trial that although he aided and abetted Mr. Brown, he did not know that the purpose of the trip was to sell methamphetamine to Ms. Stratton. Mr. Brown disputed that in his testimony. The jury ultimately convicted Mr. Finley, and he appealed the conviction.

RATIONALE

The Court found that Mr. Finley did, in fact, have standing to object to the search of his cell phone, but concluded that the search was lawful nevertheless. The court found that the search of the cell phone was allowed incident to Mr. Finley's lawful arrest.

2.4.1 - Standing to Challenge a Search of Stolen Cell Phones

In **People v. Barnes** (2013) 216 Cal.App.4th 1508, the appellate court addressed the issue of whether or not a thief has standing under the Fourth Amendment to challenge the use of a Global Positioning System (GPS) to locate a stolen cell phone and detain the thief. The court ruled that there is no Fourth Amendment violation when the information generated by the GPS, with the owner's consent, is only part of the police's objective reasons leading to their decision to detain a suspect.

FACTS (People v. Barnes (2013) 216 Cal.App.4th 1508)

Shortly after midnight on November 5, 2009, Charles Parce and Carolyn Fey were walking near Fort Mason in San Francisco when a Black male adult (later identified as Lorenzo Barnes) approached them, brandished a handgun, and demanded their belongings. Mr. Parce handed over his wallet, but Ms. Fey ran across the street and threw her turquoise Prada purse under a parked car. Mr. Barnes retrieved the purse and fled on foot. Both Mr. Parce and Ms. Fey provided a physical description of Mr.

Barnes to the police. Ms. Fey told the police that her wallet and a "Palm pre-smart phone" were inside her purse. Ms. Fey also told the police that her cell phone "had GPS on it."

Officer Zelster contacted Ms. Fey's phone service carrier, Sprint PCS, and spoke to their corporate security people. The officer was advised that if Ms. Fey would sign a release form, they would be able to ping the cell phone. What this meant is that they would be able to send a signal to the cell phone and find a general location within either 15 yards or 15 meters of the phone's location. Ms. Fey signed a release, which was faxed back to Sprint. The officer then asked Sprint to ping the cell phone and they advised the officer that the phone was stationary at 16th and Mission Street. This was approximately 45 minutes after the robbery occurred. Officer Zeltser handed the phone over to Officer Hamilton so that he could continue speaking with Sprint, while Officer Zeltser went to 16th and Mission. Enroute, Officer Zeltser learned that the ping was now "between 16th and 17th and Mission."

Officers Clifford and Tannenbaum were in the area and saw a person matching the robber's description enter a car and drive down Mission Street. While the car was stopped at a red light at 15th and Mission, the cell phone was re-pinged by Sprint and shown to be at 15th and Mission. Officer Zeltser arrived on the scene, which was now at 13th and Mission, just as Officer Tannenbaum made a car stop. As Officer Zeltser approached the car, he had his flashlight out. He looked in the rear seat of the car and saw a purse that matched Ms. Fey's description on the backseat of the car. On the front seat of the car, he saw a cell phone. It was now approximately one hour after the robbery. Once Mr. Barnes exited the car, the officers immediately noticed a gun tucked in his waistband. Ms. Fey was brought to the scene and identified Mr. Barnes as the robber. Later, at the police station, Ms. Fey identified both the purse and cell phone as her property.

Mr. Barnes brought a suppression motion challenging the legality of the initial car stop. Through his attorney, he claimed the prosecution was merely relying on a hunch and based their car stop on that hunch. He also attempted to analogize that idea to the reliability of a confidential informant and said, "I would submit that there really is not enough evidence to justify the stop of this individual miles away from where the crime occurred based upon the GPS and the clothing description, which could have fit anybody." (**Id**. at 1512.)

The trial court agreed with the prosecution's argument and stated:

> I think Ms. Fey had every right to utilize her phone company to find her phone, and I think that's what happened here. I don't believe that the defendant has a privacy interest in that regard. [¶] I don't think that there was a particular action on the part of the police . . . to intrude on the defendant's privacy. They were in pursuit of a phone that they have consent from the owner of the phone to pursue; so they went to the area where the phone was located. [¶] … [¶] I don't feel that there was an unreasonable intrusion . . . [with] . . . the stop of the defendant. [¶] Motion to suppress is denied.

(**Id**. at 1513.)

The appellate case was heard after the United States Supreme Court's decision in **United States v. Jones**. Mr. Barnes changed his argument in light of that decision and no longer saw the use of GPS technology as a per se violation of the Fourth Amendment. However, he continued to raise the issue of "reliability" and the confidential informant analogy. He also argued that even assuming that Sprint provided reliable information, "it merely established the location of the stolen phone, not the location of the suspected robber." (**Id**. at 1521.) Mr. Barnes also argued, "without the GPS information, Officers Clifford and Tannenbaum had only 'pedestrian facts—i.e., 'the suspects race, gender and attire'—'which did not support reasonable suspicion for the stop.'" (**Id**. at 1512.)

RATIONALE

After a lengthy discussion of *United States v. Jones*, the Court of Appeal said that since there was no physical trespass or intrusion, as was the case in ***Jones***, the question became one of how Mr. Barnes fared under the **Katz** [Katz v. United States (1967) 389 U.S. 347] "reasonable expectation of privacy test." In essence, the question before the court was did Mr. Barnes have a legitimate expectation of privacy in the stolen cell phone and was it one that society was prepared to recognize as reasonable. The court answered no to both questions. The court also referred to Penal Code section 637.7, which prevents law enforcement from using an electronic tracking device without the person's knowledge unless the owner of the property in question consented to the search. The court noted, "If California is willing to have police and the owner cooperate in tracking a motor vehicle, it seems unlikely state policy would be outraged by such cooperation employed to apprehend armed robbers in possession of stolen property." (**Barnes**, **supra**, at 1519.) The Court of Appeal therefore concluded that the use of GPS technology to find the location of the stolen cell phone, which assisted in locating the robber, did not violate the Fourth Amendment.

The Court of Appeal observed:

> Unlike an informant, Sprint did not initiate contact with the police. Instead, it was police, with the active assistance of the property owner, who approached Sprint. . . . The officers could verify the information passed on from Sprint if in the pinged areas the officers encountered a person matching the description provided by the victims. . . . ¶ [T]he officers could certainly infer a reasonable possibility that if they could locate the phone they would also locate the robber.

(**Id**. at 1520.)

Finally, the court concluded "[C]orrelating defendant's observed movements with both the GPS location *and* the victims' description provided Officers Tannenbaum and Clifford with ample reasonable suspicion for detention." [Citation] (**Id**.) [Italics in original.]

2.4.2 - Probable Cause and Vehicle Searches

In **Riley**, the United States proposed that the U.S. Supreme Court allow a cell phone search whenever it is reasonable to believe that the phone contains evidence of the crime for which a suspect has been arrested, based on the Court's reasoning in **Arizona v. Gant**. For example, a drug dealer who was driving a vehicle at the time of the arrest and was in possession of a cell phone.

The Court rejected this proposal and stated:

> . . . a **Gant** standard would prove no practical limit at all when it comes to cell phone searches. In the vehicle context, **Gant** generally protects against searches for evidence of past crimes. [Citation] In the cell phone context, however, it is reasonable to expect that incriminating information will be found on a phone regardless of when the crime occurred. Similarly, in the vehicle context **Gant** restricts broad searches resulting from minor crimes such as traffic violations. [Citation] That would not necessarily be true for cell phones. It would be a particularly inexperienced or unimaginative law enforcement officer who could not come up with several reasons to suppose evidence of just about any crime could be found on a cell phone. Even an individual pulled over for something as basic as speeding might well have locational data dispositive of guilt on his phone. An individual pulled over for reckless driving might have evidence on the phone that shows whether he was texting while driving. The sources of potential pertinent information are virtually unlimited, so applying the **Gant** standard to cell phones would in effect give "police officers unbridled discretion to rummage at will among a person's private effects. ([**Gant**, **supra**,] 556 U.S. at 345.)

(**Riley**, **supra**, at 2492.)

2.4.3 - Inventory Searches

Inventory searches commonly arise in the context of impounded cars, backpacks, or even luggage. However, the issue can also arise when inventorying a suspect's property at the jail prior to booking it under a suspect's name for safekeeping.

When an officer finds a cell phone inside an impounded car, and the phone is turned off—once again, given the **Riley** decision —it would be an impermissible search if the officer turned on the cell phone and examined its contents. All that is required for inventory is a notation of the cell phone make, model, and serial number. That information is usually stored in the phone's battery compartment under the battery. The contents of the cell phone would be irrelevant to the inventory search objective, and a court might view any search of those contents as a general rummaging search, which would lead to any seized evidence being suppressed.

By way of analogy, an officer who finds a briefcase in an impounded car would not be justified in reading the contents of all of the documents found in the briefcase if he was

merely filling out a simple inventory sheet. An entry of "a briefcase containing miscellaneous documents" would be sufficient.

2.4.4 - Exigent Circumstances

Even though the search incident to arrest exception does not apply to cell phones, other case-specific exceptions might still justify a warrantless search of a *particular* phone. In **Riley**, the Supreme Court observed:

> One well-recognized exception applies when 'the exigencies of the situation' make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment." [Citations.] Such exigencies could include the need to prevent the imminent destruction of evidence in individual cases, to pursue a fleeing suspect, and to assist persons who are seriously injured or are threatened with imminent injury. [Citation.]
>
> In light of the availability of the exigent circumstances exception, there is no reason to believe that law enforcement officers will not be able to address some of the more extreme hypotheticals that have been suggested: a suspect texting an accomplice who, it is feared, is preparing to detonate a bomb, or a child abductor who may have information about the child's location on his cell phone. The defendants here recognize—indeed, they stress—that such fact-specific threats may justify a warrantless search of cell phone data. See Reply Brief in No. 13–132, at 8–9; Brief for Respondent in No. 13–212, at 30, 41. The critical point is that, unlike the search incident to arrest exception, the exigent circumstances exception requires a court to examine whether an emergency justified a warrantless search in each particular case. [Citation.]

(**Riley**, **supra**, at 2494.)

2.4.5 - Abandonment

If a person abandons his or her reasonable expectation of privacy in a cell phone, even while committing a crime, then a warrantless search of the cell phone for identifying information about the owner **is permissible**. In **People v. Daggs** (2005) 133 Cal.App.4th 361, the Court of Appeal upheld the trial court's finding that the defendant had abandoned his cell phone when he left it behind at a robbery crime scene, and that the subsequent warrantless search of the cell phone by the police, which led back to the defendant, did not violate the defendant's Fourth Amendment rights.

FACTS (**People v. Daggs** (2005) 133 Cal.App.4th 361)

On December 7, 2003, the clerk at a Walgreens store in San Mateo County saw James Daggs go behind a counter and grab several cartons of cigarettes. The clerk grabbed Mr. Daggs' arm to try to stop him, but Mr. Daggs turned around, sprayed

the clerk in the eyes with pepper spray, and then fled the store with the merchandise. When the police arrived, they found a cell phone near the cash register where the clerk confronted Mr. Daggs. The clerk told the police that he had used the register 10–15 minutes before the robbery and had not seen the phone in the area. During the 20–30 minutes the police were on the premises, no one tried to claim the cell phone, so the police booked it into evidence at the police station.

One week after the robbery, no one had yet come forward to reclaim the cell phone. Detective Moran obtained the cell phone from evidence and, without a search warrant, removed the battery from the cell phone and obtained the electronic serial number, hex number, and decimal number, which were all located on the cell phone itself. Using these numbers, Detective Moran obtained a search warrant for the telephone company for the cell phone subscriber's name, phone number, and records. The documents revealed that Charles Daggs, the defendant's brother, was the subscriber. The police interviewed Charles, who told them that he had given the cell phone to his brother in August 2003, a fact that was also confirmed by the defendant's mother.

James Daggs was ultimately arrested and charged with robbery. He brought a motion to suppress the information obtained from the cell phone claiming that he had a reasonable expectation of privacy in the cell phone and that Detective Moran's search of the cell phone violated Mr. Daggs' Fourth Amendment rights. He also sought to suppress the information obtained from the search warrant on the phone company and the statements of his brother and mother as fruits of the illegal search. Mr. Daggs testified at the suppression motion that a few hours after the crime, he realized that he might have lost his cell phone at Walgreens, but decided not to try to retrieve it because he believed the police might have it and would connect him with the robbery. However, before the phone was lost, he had locked it to prevent anyone else from using it or accessing the information he stored on the cell phone.

After the trial court denied Mr. Daggs' motion, he pled no contest to one count of robbery. The court placed him on three years formal probation and sentenced him to eight months in the county jail. The Court of Appeal later upheld the trial court's decision not to suppress the seized evidence.

RATIONALE

The Court of Appeal rejected Mr. Daggs' argument and legal conclusion that because "he accidentally left his cell phone at Walgreens, and would have reclaimed it had he not feared arrest, . . . he did not voluntarily discard the phone, and therefore he did not abandon it, but merely 'lost it.'" (**Id**. at 365.) Instead, it specifically ruled that the "[d]efendant abandoned the cell phone when he left it unattended in a public place of business, at the scene of a crime, fled, and made no attempt to reclaim it." (**Id**. at 365.)

In reaching that conclusion, the court observed that the intent to abandon is determined by objective factors, and not based on a defendant's subjective intent. The Walgreens clerk

> informed the officers who found the phone at the scene that he had not seen the cell phone in that area prior to his confrontation with the robber. No one else at the scene claimed the phone, nor did anyone assert a claim to it in the week after the robbery. It was inferable that the telephone belonged to, or had been in the possession of, the robber who had fled the scene, thereby evincing his intent not to reclaim it. Therefore, when the police seized the phone, and certainly by the time Detective Moran finally performed the challenged search, these circumstances were all objective indications that defendant had discarded the phone, and would not reclaim it.

(**Id**. at 366.)

The court went on to explain that what was abandoned was the defendant's reasonable expectation of privacy in the cell phone, not necessarily the property itself. "Indeed, were it not for the incriminating circumstances, defendant, and any other reasonable person, would no doubt have hoped and expected that someone would examine the phone to ascertain the owner, and would have been grateful if someone had done so, and returned it to him." (**Id**. at 369.)

2.4.6 - Plain View Observations

Suppose an officer manipulates a cell phone to turn it off or place it in airplane mode, and in the process makes a plain view observation of something inappropriate on the cell phone such as child pornography or pictures of narcotics. Should that information be disclosed to the magistrate in a search warrant affidavit requesting authorization to search the cell phone?

The author suggests that it should not be included in the affidavit. This conclusion is based on **Segura v. United States** (1984) 468 U.S. 796, where the U.S. Supreme Court ruled that an illegal entry to secure a private residence while a search warrant was sought (it took 19 hours to get the warrant!) did not result in the suppression of evidence because the search warrant was based on independent probable cause and not on anything observed during the "freezing" of the residence. Hence, the evidence in the apartment was discovered through a lawful "independent source," that is, the search warrant.

In the context of a cell phone search warrant request, the affiant should tell the magistrate in the supporting affidavit that the cell phone was turned off, placed in airplane mode, or otherwise disconnected from the cellular network, but not told about any observations about the phone's contents the officer might have made while doing so. By not seeking a finding of probable cause based on anything

observed during the possibly inappropriate manipulating of the cell phone, a strong argument can be made that the search warrant is based on independent grounds and not on anything observed while "freezing" the cell phone. This would therefore allow one to analogize the pending case to **Segura**.

2.4.7 - Riley and the Future of Cell Phone Searches

Technology continues to evolve and converge in this area, as cell phones become more like handheld computers and less like traditional phones. Because of this evolving situation, the day may arise when a court rules that cell phone searches should be governed by alternative statutory schemes (e.g., the PPA), rather than by traditional Fourth Amendment analysis. (See Justice Alito's concurring opinion in **Riley**.) Officers should always remember that bad facts can create bad rules of law, and that it is prudent to carefully consider a situation before searching through information stored on a cell phone. **When in doubt, always get a search warrant.**

2.4.8 - Consent

Warrantless searches based on consent are almost always legal. However, there are four basic questions to consider when analyzing the lawfulness of a search based on consent:

1. Was there consent?
2. Was the consent freely and voluntarily given?
3. Did the consenting party have the authority to give consent?
4. What was the scope of the consent?

2.4.8.1 - General Rules

The U.S. Supreme Court ruled in **Schneckloth v. Bustamonte** (1973) 412 U.S. 218, that the police do not have to tell a subject who voluntarily consents to a search that he or she has the right to withhold consent. However, it is a proper factor to look at when considering whether the person freely and voluntarily consented to the search.

In **United States v. Matlock** (1974) 415 U.S. 164, 171, the U.S. Supreme Court ruled that no warrant is needed if a competent individual who "possessed common authority over or other sufficient relationship to the premises or effects sought to be inspected. . ." consents to the search.

Under **Matlock**, common authority rests on mutual use of the property by persons generally having joint access or control for most purposes. The burden for proving that common authority rests on the State.

However, in a 5–3 decision written by Justice Souter in **Georgia v. Randolph** (2006) 547 U.S. 103, the U.S. Supreme Court ruled that the Fourth Amendment provisions against unreasonable searches and seizure are violated when police conduct a warrantless search of a residence based on the consent of one occupant when a co-occupant is present and objects to the search. The Court ruled that the fruits of such a warrantless

search are inadmissible against the physically present, non-consenting party. In reaching this decision, the Court observed,

> [T]here is no common understanding that one co-tenant generally has a right or authority to prevail over the express wishes of another, whether the issue is the color of the curtains or invitations to outsiders.

(**Id**. at 114.)

In reaching this conclusion, the majority had to justify its decision in light of its own precedent in **Matlock**, where it upheld the entry to a residence based on the consent of one co-occupant in the absence of the other. Justice Souter referred to this as "two loose ends," which he characterized as:

1. The explanation "for the constitutional sufficiency of a co-tenant's consent to enter and search" in **Matlock**.
2. The significance of **Matlock** and **Illinois v. Rodriguez** (1990) 497 U.S. 177 after the U.S. Supreme Court's decision in this case.

Justice Souter explained away the first issue by stating that the **Matlock** Court did not address the issue of "whether customary social understanding accords the consenting tenant authority powerful enough to prevail over the co-tenant's objection."

(**Randolph**, **supra**, at 121.)

With respect to the second issue, Justice Souter said:

> If those cases are not to be undercut by today's holding, we have to admit that we are drawing a fine line; if a potential defendant with self-interest in objecting is in fact at the door and objects, the co-tenant's permission does not suffice for a reasonable search, whereas the potential objector, nearby but not invited to take part in the threshold colloquy, loses out.
>
> This is the line we draw, and we think the formalism is justified. So long as there is no evidence that the police have removed the potentially objecting tenant from the entrance for the sake of avoiding a possible objection, there is practical value in the simple clarity of complementary rules, one recognizing the co-tenant's permission when there is no fellow occupant on hand, the other according dispositive weight to the fellow occupant's contrary indication when he expresses it.

(**Id**. at 121.)

In a strong dissent, Chief Justice Roberts disagreed with the majority rule and stated:

> A wide variety of often subtle social conventions may shape expectations about how we act when another shares with us what is otherwise private, and those conventions go by a variety of labels—courtesy, good manners, custom, protocol, even honor among thieves. The Constitution, however, protects not these but privacy, and once privacy has been shared, the shared information, documents, or places remain private only at the discretion of the confidant.

(**Id**. at 131.)

The Chief Justice expressed his belief that the majority's decision did not protect privacy nearly as much as the good luck of a co-owner who just happened to be present when the police arrived at the door.

Finally, the Chief Justice argued:

> [T]he more reasonable approach is to adopt a rule acknowledging that shared living space entails a limited yielding of privacy to others, and that the law historically permits those to whom we have yielded our privacy to in turn cooperate with the government. Such a rule flows more naturally from our cases concerning Fourth Amendment reasonableness and is logically grounded in the concept of privacy underlying that Amendment.

(**Id**. at 137.)

In **People v. Fernandez** (2014) ___ U.S. ___; 134 S.Ct. 1126, the U.S Supreme Court followed the holding in **Georgia v. Randolph**, **supra**, and upheld the co-tenants' consent to search the apartment despite the fact that Mr. Fernandez objected to such a search before he was lawfully arrested and removed from the premises.

In the case of **In re D.C.** (2010) 188 Cal.App.4th 978, the Court of Appeal concluded that "[b]ecause of the unique nature of the rights and duties of parents with respect to their children, **Randolph** does not require the police to defer to an objecting minor child over a consent to search by his or her parent." (**Id**. at 989.)

Officers need to proceed with extreme caution when attempting to search a cell phone or even a computer in a **Georgia v. Randolph** type of situation. The consent of a spouse or co-occupant who has joint access and control over a cell phone or computer will not be sufficient if the other spouse or co-occupant is present and objects to the search. A search done over the objections of a present spouse or co-occupants could lead to the suppression of any evidence obtained during that cell phone or computer search.

2.4.8.2 - Parents and Children

In **In re Scott K.** (1979) 24 Cal.3d 395, the California Supreme Court ruled that the minor's father could not lawfully give the police consent to search a locked toolbox inside the room of his 17-year-old son because the father claimed no interest in the son's locked tool box or its contents and acknowledged that the toolbox belonged to his son.

In reaching that conclusion, the California Supreme Court rejected the following arguments put forth by the People in support of the police search:

- Because a parent is responsible for minor children and may inspect their property on their own, the police search was lawfully based on the parental consent.
- The father's consent fell within a third party exception to the warrant requirement based on the combined circumstances of ownership of the home and the nature of the parent-child relationship.

The Court of Appeal ruled in **People v. Daniels** (1971) 16 Cal.App.3d 36, that Mr. Daniels's mother could properly give the police consent to search her adult son's bedroom for evidence of bomb making materials when the son resided at the house rent free. However, she could not give the police consent to search a suitcase in the bedroom that belonged to her son.

With respect to cell phone searches, a parent who has no access to or right of control over a minor child's cell phone would not be able to lawfully consent to a search. Likewise, even if a parent pays the cell phone bill for an adult child, but otherwise does not share or use that adult child's cell phone, the parent would not have the authority to give law enforcement consent to search it.

2.4.8.3 - Third Parties

In a 6–3 decision in **Illinois v. Rodriguez** (1990) 497 U.S. 177, the Supreme Court ruled that a warrantless entry does not violate the Fourth Amendment proscription against unreasonable searches and seizures where such entry is based upon the consent of a third party, whom the police, at the time of entry, reasonably believe to possess common authority over the premises, but who in fact does not possess such authority.

The Court applied the following objective test:

> Whether the facts available at the moment would warrant a person of reasonable caution in the belief that the consenting party had authority over the premises. If not, then warrantless entry without further inquiry is unlawful unless authority actually exists. But if so, the search is valid.

(**Id**. at 178.)

In the context of cell phone searches, if the officers reasonably believe that the consenting party has sole control, ownership, and use of the cell phone, but it later turns out that they were lied to, the search should be upheld based on the holding in **Illinois v. Rodriguez**.

2.4.8.4 - Landlords

In **Chapman v. United States** (1961) 365 U.S. 610, the U.S. Supreme Court ruled in an 8–1 decision that a landlord cannot give the police consent to enter a tenant's residence. By way of analogy, a landlord also cannot give police consent to search a tenant's cell phone.

2.4.9 - Probation Searches

2.4.9.1 - General Principles

Probation searches—when there is a search and seizure clause associated with the grant of probation—are generally going to be upheld by the courts' under the "special needs" doctrine articulated by the 5–4 U.S. Supreme Court decision in *Griffin v. Wisconsin* (1987) 483 U.S. 868. It does not matter if the search is for investigatory purposes or probationary purposes. Furthermore, a probation search conducted pursuant to a

known probation condition, even without a reasonable suspicion of criminal activity, will be upheld, provided the search is not done for arbitrary, capricious, or harassment purposes.

In recognizing the validity of warrantless probation searches in **Griffin, *supra,*** at 876, the Court stated,

> [a] warrant requirement would interfere to an appreciable degree with the probation system, setting up a magistrate rather than the probation officer as the judge of how close a supervision the probationer requires. Moreover, the delay inherent in obtaining a warrant would make it more difficult for probation officials to respond quickly to evidence of misconduct, see **New Jersey v. T.L.O**. (1985) 469 U.S. 325, at 340, and would reduce the deterrent effect that the possibility of expeditious searches would otherwise create, [citations]. By way of analogy, one might contemplate how parental custodial authority would be impaired by requiring judicial approval for [the] search of a minor child's room.

In reaching this decision, the U.S. Supreme Court declined to embrace the Wisconsin Supreme Court's new principle of law that ". . . any search of a probationer's home by a probation officer satisfies the Fourth Amendment as long as the information possessed by the officer satisfies a federal 'reasonable grounds' standard." (**Id**. at 872.) Instead, the U.S. Supreme Court upheld the constitutionality of the search based on "special needs" beyond normal law enforcement. Those "special needs" justified a departure from the usual probable cause and warrant requirements.

In **United States v. Knights** (2001) 534 U.S. 112, the U.S. Supreme Court unanimously reversed the Ninth Circuit Court of Appeals and held that the search of Mr. Knights pursuant to his probation condition and supported by reasonable suspicion, did not violate the Fourth Amendment. In doing so, the Supreme Court specifically rejected the Ninth Circuit's distinction that the search was illegal because it was done for an investigatory purpose rather than a probationary purpose.

In **People v. Medina** (2007) 158 Cal.App.4th 1571, the Court of Appeal reversed the trial court's decision and explicitly ruled that under California law and the California Supreme Court's decision in **People v. Bravo** (1987) 43 Cal.3d 600,

> . . . a search conducted pursuant to a known probation search condition, even if conducted without reasonable suspicion of criminal activity, does not violate the Fourth Amendment as long as the search is not undertaken for harassment or for arbitrary or capricious reasons or in an unreasonable manner.

(**Medina**, **supra**, at 1577.)

The Court of Appeal also noted that

> [the] . . . ***Knights*** court expressly declined to reach the issue whether "acceptance of the search condition constituted consent in the ***Schneckloth*** sense of a complete waiver of his Fourth Amendment rights." (**Knights**, **supra**, 534 U.S. at p. 118.) Moreover, the court expressly declined to decide whether a probation search

> *without* reasonable suspicion satisfies the reasonableness requirement of the Fourth Amendment. (**Knights**, **supra** at p. 120, fn. 6.) Thus, **Knights** did not consider the question relevant to the present case: whether reasonable suspicion is *required* (and not just sufficient) for a search pursuant to a probation condition. [Italics in original.]

(**Medina**, **supra**, at 1578.)

There is no reasonableness requirement before an officer can conduct a probation search. All that is required is that the search is not arbitrary, capricious, or done for harassment purposes (see **In re Anthony S.** (1992) 4 Cal.App.4th 1000, 1004) and an officer's subjective intentions play no role in determining the lawfulness of a probation or parole search.

> As explained in **People v. Clower** (1993) 16 Cal.App.4th 1737 [21 Cal.Rptr. 2d 38], "a parole search could become constitutionally 'unreasonable' if made too often, or at an unreasonable hour, or if unreasonably prolonged or for other reasons establishing arbitrary or oppressive conduct by the searching officer." (*Id*. at 1741; **United States v. Follette** (S.D.N.Y. 1968) 282 F.Supp.10, 13; see **In re Anthony S**., (1992) 4 Cal.App.4th 1000, 1004 [6 Cal.Rptr.2d 214] [a search is arbitrary and capricious when the motivation for the search is unrelated to rehabilitative, reformative or legitimate law enforcement purposes, or when the search is motivated by personal animosity toward the parolee]; **People v. Bremmer** (1973) 30 Cal.App.3d 1058, 1062 [106 Cal.Rptr. 797] [unrestricted search of a probationer or parolee by law enforcement officers at their whim or caprice is a form of harassment].)

People v. Reyes (1998) 19 Cal.4th 743, at 753–754.

In **People v. Sardinas** (2009) 170 Cal.App.4th 488, the Court of Appeal rejected Mr. Sardinas's contention that the two searches occurring within 24 hours of each other, combined with the officer's prior six or seven contacts with him over a five-year period, belied any legitimate purpose for the second search that resulted in the seizure of cocaine from his person, and compelled the conclusion that the search was done for harassment or other arbitrary purpose.

In **People v. Gomez** (2005) 130 Cal.App.4th 1008, the Court of Appeal ruled that an " officer's subjective intent has no role to play in determining the lawfulness of a probation or parole search."

(**Id**. at 1015.)

2.4.9.2 - Scope of Search

In **People v. Ermi**, (2013) 216 Cal.App.4th 277, the Court of Appeal addressed the issue of whether a probationer's search condition authorized the search of a purse belonging to the probationer's girlfriend that the officer found on a chair in a shared bedroom. The Court of Appeal upheld the trial court's ruling that the officer properly searched the purse because the probationer had access and control over the purse.

Likewise, if a probationer has access and control over a cell phone, a probation search of the cell phone under these circumstances should be upheld by the courts.

2.4.9.3 - Cohabitant Search Conditions

In a 6–1 decision, **People v. Sanders** (2003) 31 Cal.4th 318, 335, with only Associate Justice Baxter dissenting, the California Supreme Court repudiated the rationale of **In re Tyrell J.**, **supra**, in the context of parole searches. The Court held that

> . . . an otherwise unlawful search of the residence of an adult parolee may not be justified by the circumstance that the suspect was subject to a search condition of which the law enforcement officers were unaware when the search was conducted.

In his majority opinion, Justice Moreno stated,

> [p]ermitting evidence that has been suppressed as to a cohabitant to be used against the parolee would encourage searches that violate the rights of cohabitants and guests by rewarding police for conducting an unlawful search of a residence.

Sanders, **supra**, at 335.

A search that violates a cohabitant's reasonable expectation of privacy also violates a parolee's expectation of privacy. While ". . . a parolee's expectation of privacy is certainly diminished, it is not eliminated." **Sanders**, **supra**, at 332.

By suppressing the evidence against both defendants, the Supreme Court sent a clear signal to law enforcement that it did not want to legitimize the police's illegal actions.

The California Supreme Court later applied the same rule to probation searches for their decision in **In re Jaime P**. (2006) 40 Cal.4th 128.

In **People v. Pleasant** (2004) 123 Cal.App.4th 194, the Court of Appeal upheld the search of a locked bedroom in a probationer's (mom) house and the subsequent seizure of firearms used against her adult son in a criminal prosecution. Even though the son resided in that bedroom, the probationer possessed keys to that locked bedroom.

The majority observed:

> Persons who live with probationers cannot reasonably expect privacy in areas of a residence that they share with probationers. (**People v. Woods** (1999) 21 Cal.4th 668, 675–676.) Since Ms. Pleasant gave a search waiver as a condition of probation, law enforcement authorities could, without a warrant or probable cause, search areas used exclusively by Ms. Pleasant, areas within "common authority" . . . of the probationer and fellow occupants and areas which she "normally had access." [Citations.] Since Ms. Pleasant had access to the keys to the room in which the gun was found, [Mr.] Pleasant could not reasonably expect privacy in the room and the officers reasonably entered the room under the authority of Ms. Pleasant's probation waiver.
>
> (**Pleasant**, **supra**, at 197–198.)

In this 2–1 decision, the dissenting justice noted that the officers were told the room belonged to the probationer's son and that he kept the door locked. Based on this information, the dissenting Justice believed the officers could not reasonably believe Ms. Pleasant had access to this clearly "differentiated private living space."

2.4.9.4 - Probation Searches and Electronic Devices

Given our technological society and the proliferation of computers, electronic storage devices such as cell phones, personal digital assistants (PDAs) and thumb drives, the issue often arises as to whether an officer can conduct a warrantless search of a probationer's computer and other electronic items as part of a probation search. The answer to this question is a qualified maybe.

If a probationer is on probation for a crime involving the use of a computer, the trial court may have ordered restrictions on the probationer's use and possession of computer equipment. For example, Penal Code section 1203.047 mandates that a person convicted of a violation of certain subdivisions of Penal Code sections 502 or 502.7 be placed on not less than three years of probation unless the ends of justice would be served by a shorter term. Section 1203.047 also mandates that

> During the period of probation, that person shall not accept employment where that person would use a computer connected by any means to any other computer, except upon approval of the court and notice to and opportunity to be heard by the prosecuting attorney, probation department, prospective employer, and the convicted person. Court approval shall not be given unless the court finds that the proposed employment would not pose a risk to the public.

A probationer's mere possession of a computer under those circumstances would be a violation of the terms of probation and would justify its search and seizure by law enforcement.

A sentencing court may also impose other restrictions such as specific terms allowing search and seizure of all digital devices in a probationer's possession, including both on-site and off-site analysis by a forensic lab. Such a condition would obviously justify the warrantless seizure, removal, and off-site forensic analysis by a lab of a computer or cell phone and its contents.

However, if the sentencing court did not go so far in issuing probation conditions, but instead issued terms of probation that included stay away orders from online computer chat rooms, a prohibition against the use of pseudonyms in online communications, no credit card use over the Internet, and no participation in Internet-based auctions or e-commerce, then the situation moves into a gray area.

Once law enforcement verifies some or all of the above probation conditions, a probationer's Fourth Amendment rights would not be violated if an officer conducted a warrantless search of a probationer's computer files, cell phone information, or PDA either at or away from the location of the probation search.

In the absence of those conditions, a very cursory search of electronic items for evidence of dominion and control of the property would be appropriate. For a more detailed search, including removing the computer or cell phone for analysis at a forensic lab, the better practice is to freeze the device and promptly obtain a search warrant allowing it to be removed from the location. For example, if the court prohibits a probationer from possessing child pornography and a probation officer's cursory search of a computer or cell phone yields evidence of the presence of picture files containing such items, the officer should seize the device and suspend any further search pending the issuance of a search warrant authorizing a more detailed off-site forensic analysis of its information.

2.4.10 - Parole Searches

Parole searches are very similar to probation searches, but almost always include a search and seizure clause. Penal Code section 3067, when enacted in 1996, initially required an inmate to consent to a search and seizure condition in exchange for being released from prison. However, in 2012, the California Legislature amended the section in response to prison overcrowding and the enactment of Penal Code section 1170(h), which allows prison sentences to be served in local county jails. Under the revised formulation, a parolee was only required to be advised that he or she is subject to search and seizure by probation, parole, or peace officers at any time of the day or night, with or without a search warrant or with or without probable cause. In 2006, the U.S. Supreme Court ruled that a suspicionless search of a parolee did not violate the Fourth Amendment prohibition against unreasonable searches and seizures.

The California Legislature added Penal Code section 3067 in 1996. At that time, subdivision (a) mandated that

> Any inmate who is eligible for release on parole pursuant to this chapter shall agree in writing to be subject to search or seizure by a parole officer or other peace officer at any time of the day or night, with or without a search warrant and with or without cause.

Subdivision (b) stated that "Any inmate who does not comply with the provision of subdivision (a) . . . shall not be released until he or she either complies with the provision of subdivision (a) or has no remaining worktime credit, whichever occurs earlier."

In passing this legislation, the California Legislature limited its application in subsection (c) "This section shall only apply to an inmate who is eligible for release on parole for an *offense committed on or after January 1, 1997*."

In 2012, the California Legislature amended Penal Code section 3067 to eliminate the language in subdivision (a) requiring an inmate to agree in writing to be subject to search or seizure by a parole officer or other peace officer at any time of the day or

night. The amendment added paragraphs (1), (2), and (3) to subdivision (b). The amended statute now reads in part as follows:[8]

> (a) Any inmate who is eligible for release on parole pursuant to this chapter or postrelease community supervision pursuant to Title 2.05 (commencing with Section 3450) of Part 3 shall be given notice that he or she is subject to terms and conditions of his or her release from prison.
>
> (b) The notice shall include all of the following:
>
> (1) The person's release date and the maximum period the person may be subject to supervision under this title.
>
> (2) An advisement that if the person violates any law or violates any condition of his or her release that he or she may be incarcerated in a county jail or, if previously paroled pursuant to Section 3000.1 or paragraph (4) of subdivision (b) of Section 3000, returned to state prison, regardless of whether new charges are filed.
>
> (3) An advisement that he or she is subject to search or seizure by a probation or parole officer or other peace officer at any time of the day or night, with or without a search warrant or with or without cause.
>
> (c) This section shall only apply to an inmate who is eligible for release on parole for an offense committed on or after January 1, 1997.
>
> (d) It is not the intent of the Legislature to authorize law enforcement officers to conduct searches for the sole purpose of harassment.

The California Supreme Court initially applied its decision in **In re Tyrell J.**, supra, to parole searches in a 4–3 decision in **Reyes**, **supra**, 19 Cal.4th 743 and in so doing, disapproved its earlier decisions in **In re Ralph Martinez** (1970) 1 Cal.3d 641, which held that a warrantless search of a residence could not be upheld as a parole search, if the officers were unaware of the parole condition at the time they conducted the search—and **People v. Burgener** (1986) 41 Cal.3d. 505, which held that a warrantless search of a parolee must be justified by at least a reasonable suspicion that the parolee had violated a condition of his parole or a law, or was planning to do so. However, as stated earlier, the California Supreme Court reversed itself in *Sanders*, *supra*, 31 Cal.4th 318, just five years later, which means that **In re Ralph Martinez** and **People v. Burgener** are once again valid California law.

In **People v. Middleton** (2005) 131 Cal.App.4th 732, the Court of Appeal ruled that an officer's awareness that a third party was a parolee was sufficient to inform the officer

[8] All new additions are shown as underlined text. Additionally, only subsection (e), which relates to the power of the Secretary of Department of Corrections and Rehabilitation to prescribe and amend rules and regulations, is omitted above.

of the existence of a search and seizure clause (see Penal Code 3067(a)) and provide the officer with authority to conduct a warrantless search of a motel room.

In a 6–3 opinion in **Samson v. California** (2006) 547 U.S. 843, the U.S. Supreme Court resolved the question it left open in **United States v. Knights** (2001) 534 U.S. 112:

> whether a condition of release can so diminish or eliminate a released prisoner's reasonable expectation of privacy that a suspicionless search by a law enforcement officer would not offend the Fourth Amendment.

Samson, **supra**, at 847.

The Court ruled that suspicionless searches of a parolee do not violate the Fourth Amendment prohibition against unreasonable searches and seizures. Based on Proposition 8, California courts are bound to follow this decision. This means that **Samson** supersedes the California Supreme Court's decision in **Burgener**, **supra**, requiring a "reasonable suspicion" standard before an officer can search a parolee.

2.4.10.1 - Invalidity of Parole Search Conditions

The issue often arises as to when a suspect, who is on parole, can no longer be searched based on the parole conditions because the parolee has been incarcerated for a parole violation. In **People v. Hunter** (2006) 140 Cal.App.4th 1147 (cert. denied, March 19, 2007, 127 S.Ct. 1838), the Court of Appeal held that a parole officer retained authority to conduct a parole search of Mr. Hunter before the court formally revoked his parole.