RECENT DEVELOPMENTS IN DIGITAL PRIVACY: FOURTH AMENDMENT AND PROBATION CONDITIONS

By: Nerissa Huertas

Recent Developments in Digital Privacy: 4th Amendment & Probation Conditions

By Nerissa J. Huertas, Staff Attorney
Sixth District Appellate Program

Introduction

In addressing digital privacy issues, this article begins with the Supreme Court's decision in *Riley v. California* (2014) 134 S.Ct. 2473 because that decision outlined, in sweeping language, the privacy issues at stake in the government's potential to search our digital devices. *Riley* was significant in emphasizing that our rapidly expanding world of technological advances may very well call for new legal analyses. As noted by Justice Kline of the First District, "The Supreme Court's analysis in *Riley* highlight[ed] the dangers inherent in lawyers and judges cavalierly applying established legal theories to new technologies, without carefully exploring the factual differences between such technologies and the objects traditionally found appropriate for those theories' application." (*People v. Michael E.* (2014) 230 Cal.App.4th 261, 277.)[1]

Part I offers an overview of the Supreme Court's opinion in *Riley*, before discussing California and Ninth Circuit cases applying *Riley* to different legal and factual circumstances. The section then highlights other areas of Fourth Amendment jurisprudence that may be affected by the holding in *Riley*.

Part II provides an overview of the recently-enacted California Electronic Communications Privacy Act. (Pen. Code, Ch. 3.6, added by Stats. 2015, Ch. 651.)

Part III addresses electronic search probation conditions and other conditions affecting digital privacy rights. The section first provides an overview of recent Court of Appeal cases addressing privacy rights post-*Riley*. The section next highlights a number of legal claims that may be overlooked, but can be raised, when challenging such probation conditions.

Finally, Part IV provides examples and illustrations of terms commonly used when discussing issues of digital privacy.[2]

---

[1] Because this article approaches the issue of digital privacy wholly through the prism of *Riley*, it necessarily excludes some relevant cases both pre- and post-*Riley*. It should, however, get you where you need to go.

[2] This article does not address the FBI's recent battle with Apple. If you are interested in learning more about the FBI's battle, and the ongoing encryption/backdoor debate, please watch this great overview of the issue, provided by Last Week Tonight with John Oliver: Encryption (HBO), found at < https://www.youtube.com/watch?v=zsjZ2r9Ygzw> [as of March 28, 2016].

I. The Fourth Amendment and Electronic Searches After *Riley v. California.*

a. *Riley v. California*

On June 25, 2014, the Supreme Court issued a unanimous opinion in companion cases *Riley, supra,* 134 S.Ct. 2473 and *United States v. Wurie*, written by Chief Justice Roberts, with a concurring opinion by Justice Alito. Both cases presented the question of whether "the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested." (*Id.* at p. 2480; see also Butler, *Get a Warrant: The Supreme Court's New Course for Digital Privacy Rights After Riley v. California* (2014) 10 Duke J. Const. Law & Pub. Pol'y 83, 84-93 [analysis of *Riley*].) The Court held that the warrantless search of a cell phone seized during a lawful arrest was unreasonable and violated the Fourth Amendment.

To begin its analysis, the Supreme Court noted that the "ultimate touchstone of the Fourth Amendment is 'reasonableness'" and that, under the reasonableness standard, a search "undertaken by law enforcement officials to discover evidence of criminal wrongdoing" generally requires "the obtaining of a judicial warrant." (*Riley*, *supra*, 134 S.Ct. at p. 2482.) The Court further explained that in the absence of a warrant, a search is only reasonable "if it falls within a specific exception to the warrant requirement"—one of which allows a search "of the accused when legally arrested to discover and seize the fruits or evidences of crime." (*Ibid.*)

The Court had previously established the boundaries of the search-incident-to-arrest exception in three cases: *Chimel v. California* (1969) 395 U.S. 752, *United States v. Robinson* (1973) 414 U.S. 218, and *Arizona v. Gant* (2009) 556 U.S. 332. In *Chimel*, the Court held that there was "ample justification . . . for a search of the arrestee's person and the area 'within his immediate control'—construing that phrase to mean the area from within which he might gain possession of a weapon or destructible evidence." (*Chimel*, *supra*, 395 U.S. at pp. 762-763.) The justification for this exception was twofold: (1) to protect the arresting officer and prevent escape; and (2) to prevent the concealment or destruction of evidence. (*Ibid.*)

The Court later clarified this rule in *Robinson*, finding that the physical inspection of an object discovered during the search of the arrestee's person is permissible, regardless of "the probability in a particular arrest situation that weapons or evidence would in fact be found upon the person of the suspect." (*Robinson*, *supra*, 414 U.S. at p. 235.) As the Court noted in *Robinson*, this rule was largely pragmatic: "A police officer's determination as to how and where to search the person of a suspect whom he has arrested is necessarily a quick ad hoc judgment which the Fourth Amendment does not require to be broken down in each instance into an analysis of each step in the search." (*Ibid.*) In *United States v. Chadwick* (1977) 433 U.S. 1, however, the Court clarified that the *Robinson* rule did not apply to physical containers that were "not immediately associated with the person of the arrestee." (*Id.* at p. 15 [holding a locked footlocker could not be searched incident to arrest].)

Later, in *Gant*, the Court applied the *Chimel* rule to the search of a vehicle and found that police could search a vehicle under the exception "only when the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search." (*Gant*, *supra*, 556 U.S. at p. 343.) However, the Court found that a separate exception would allow for the search of a vehicle "when it is 'reasonable to believe evidence related to the crime of arrest might be found in the vehicle.'" (*Ibid.*)

Prior to *Riley*, lower courts applying the rules in *Chimel* and *Robinson* were split over whether the exception permitted officers to search photos, call logs, messages, and other data stored on a cell phone. Some courts viewed this as a straightforward application of *Robinson*—any phone found within the arrestee's zone of control could be searched and inspected without further justification. (See, e.g., *Diaz*, *supra*, 244 P.3d at p. 510.) Other courts disagreed, however, finding that the *Chimel* justifications were not applicable to the search of digital files stored on a cell phone—those files did not pose a threat to the officer and there was no risk of loss of evidence once the phone had been secured. (See, e.g., *United States v. Wurie* (1st Cir. 2013) 728 F.3d 1, 11.)

In a unanimous opinion, the Court held that cell phones must be subject to different rules than other physical objects within the search-incident-to-arrest exception. (*Riley*, *supra*, 134 S.Ct. at pp. 2490-2491.) Thus, although the default rule for inspection of physical objects under *Robinson* had been that no warrant is required for a physical search incident to arrest (*Robinson*, *supra*, 414 U.S. at p. 235), the default rule for cell phones under *Riley* is "get a warrant." (*Riley*, *supra*, 134 S.Ct. at p. 2495.)

The Court noted that digital devices are fundamentally different than physical objects. Whereas physical searches had traditionally been "limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy," cell phones can contain "millions of pages of text, thousands of pictures, and hundreds of videos." (*Riley*, *supra*, 134 S.Ct. at p. 2489.)

The Court further addressed the "interrelated consequences for privacy" of the increasing storage capacity of mobile devices, which enables the consolidation of many different types of information that could "reveal much more in combination than any isolated record." (*Riley*, *supra*, 134 S.Ct. at p. 2489.) The Court also noted that the aggregation of photos or other files, along with timestamps and associated metadata, would reveal a great deal more than individual physical items ever could. (*Ibid.*) Similarly, the archival nature of stored data, providing a record that traces back to the purchase of the phone and potentially beyond, makes a search of the digital device much more invasive than a search of the physical object. (*Ibid.*) And finally, the Court concluded that the pervasiveness of modern cell phones, which most users now carry with them at all times, means that the privacy cost of allowing routine searches of cell phones is much greater than the cost of "allowing them to search a personal item or two in the occasional case." (*Id.* at p. 2490.)

The Court went on to emphasize that highly sensitive records are now routinely stored on mobile phones, and that these records are "qualitatively different" from what

would have been available during a physical search. The Court found that the highly sensitive data includes "Internet search and browsing history," "[h]istoric location information," "transaction records," as well as data from a variety of new mobile "apps" that relate to private activities and interests." (*Riley*, *supra*, 134 S.Ct. at p. 2490.) Cell phones contain such a wealth of data, the Court reasoned, that "a cell phone search would typically expose the government to far *more* than the most exhaustive search of a house." (*Ibid.*) Cell phones also provide access to sensitive personal information stored on remote servers, and law enforcement would have no clear way to distinguish between locally and remotely stored data. (*Id.* at p. 2491.)

Significantly, the Court considered, and rejected, various alternative standards offered by the Government, finding that those posited alternative standards would impose no meaningful limitations on cell phone searches and would be impractical to administer. (*Riley*, *supra*, 134 S.Ct. at pp. 2491-2493.) The United States had proposed that the Court adopt the "*Gant* standard" and allow officers to search cell phones "whenever it is reasonable to believe that the phone contains evidence of the crime of arrest." (*Id.* at p. 2492.) The United States had alternatively proposed that an officer should be allowed to search the phone when she "reasonably believes that information relevant to the crime, the arrestee's identity, or officer safety will be discovered." (*Ibid.*) And finally, the United States had suggested that officers should at least be allowed to search an arrestee's cell phone "call log." (*Id.* at pp. 2492-2493.) California had suggested "a different limiting principle, under which officers could search cell phone data if they could have obtained the same information in a pre-digital counterpart." (*Id.* at p. 2493.)

The Court acknowledged that its decision "will have an impact on the ability of law enforcement to combat crime," but noted that "[p]rivacy comes at a cost." (*Riley*, *supra*, 134 S.Ct. at p. 2493.) The warrant requirement is "not merely 'an inconvenience to be somehow weighted against the claims of police efficiency.'" (*Ibid.*) Instead, the Fourth Amendment is a critical safeguard, "the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." (*Id.* at p. 2494.) The Court ended by noting that opposition to warrantless search "was in fact one of the driving forces behind the [American] Revolution," and that John Adams had described a speech by James Otis decrying writs of assistance as "the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born." (*Ibid.*) The Court then emphasized that, "Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'" (*Id.* at pp. 2494-2495.)

b. California Cases Applying *Riley*

i. *People v. Macabeo* (2014) 229 Cal.App.4th 486-Superseded by Grant of Review

In *People v. Macabeo* (2014) 229 Cal.App.4th 486, defendant was riding his bicycle at 1:40 a.m. in Torrance, California, when, riding directly in front of a police vehicle, he rolled through a stop sign without slowing down. (*Id.* at p. 489.) Police officers stopped defendant, learned that he was possibly on probation for "methamphetamine," and one of the officers initiated a patdown search, before asking defendant for consent to search his pockets. (*Ibid.*) Defendant agreed, and the officer removed, amongst other items, a cell phone from defendant's pocket. (*Ibid.*) Upon searching the cell phone, officers discovered no text messages concerning narcotics, but found a picture folder on the phone that contained pictures of young girls under the age of 18 engaged in sexual activity. (*Ibid.*) Defendant was then placed under arrest. (*Ibid.*) Defendant was not, in fact, on felony probation at the time of his arrest. (*Ibid.*)

Defendant was charged with possession of matter depicting a minor engaging in sexual conduct, in violation of Penal Code section 311.11, subdivision (a),[3] and with possession of a smoking device, in violation of Health & Safety Code section 11364.1, subdivision (a)(1). (*Macabeo*, *supra*, 229 Cal.App.4th at pp. 489-490.) Defendant filed a motion to suppress evidence, pursuant to section 1538.5, contending that the pictures on his cell phone had been obtained during an unlawful search and seizure. (*Id.* at p. 490.) The court denied the suppression motion and held defendant to answer. (*Ibid.*) Following the denial of a renewed suppression motion, defendant ultimately pleaded no contest to a violation of section 311.11, subdivision (a). (*Ibid.*)

Defendant appealed from the trial court's order denying his motion to suppress evidence, and argued that the trial court had erred in finding the search of his cell phone, incident to a stop for a minor traffic violation permissible, under the Fourth Amendment. (*Macabeo*, *supra*, 229 Cal.App.4th at p. 494.) While *Macabeo* was on appeal, the Supreme Court overruled *Diaz*, *supra*, 51 Cal.4th 84, with its holding in *Riley*, *supra*, 134 S.Ct. 2473. (*Id.* at pp. 491-492.) Nevertheless, the Second District Court of Appeal held that, because *Diaz* had been applicable at the time of the search, the officers' conduct in searching the cell phone fell within the good faith exception to the exclusionary rule and, thus, the failure to exclude the evidence from the cell phone was not reversible error. (*Id.* at pp. 495-497.)

The California Supreme Court granted review in *Macabeo* on November 25, 2014. (*People v. Macabeo* (2014) 338 P.3d 938.) The Court of Appeal opinion has therefore been depublished.

---

[3] Subsequent section references are to the Penal Code, unless otherwise indicated.

ii. *People v. Michael E.* (2014) 230 Cal.App.4th 261

The defendant in *People v. Michael E.* (2014) 230 Cal.App.4th 261 had brought his computer to a repair shop for servicing. (*Id.* at p. 264.) In the course of working on the computer, the repair person viewed images on the computer of what appeared to him to be underage girls engaged in sexual activity. (*Ibid.*) After notifying the police, an officer viewed the files at the computer repair shop and noted that, although the girls in the photos were posing in a sexual manner, none of the images were pornographic. (*Ibid.*)

The officer asked the repair person to "search through and look at" anything else in the computer. (*Michael E.*, *supra*, 230 Cal.App.4th at p. 264.) Upon further examination, the repair person found video files on the computer that he was unable to open, but he put the video files on a USB flash drive that he gave to the officer. (*Ibid.*) A police sergeant was ultimately able to open the files and, after finding "juvenile pornographic material," defendant's computer was seized. (*Ibid.*) The police never obtained a search warrant. (*Id.* at p. 265.) Defendant was charged with felony possession of material depicting a minor engaging in or simulating sexual conduct (§ 311.1, subd. (a)). (*Id.* at p. 264.)

Defender filed a motion to suppress evidence seized from his computer. (*Michael E.*, *supra*, 230 Cal.App.4th at p. 264.) In response, the prosecution argued that: (1) because the evidence was not obtained from the repair person illegally, the Fourth Amendment did not apply; and (2) defendant's expectation of privacy was destroyed once a private citizen made the search and revealed his findings to the police. (*Ibid.*)

After defendant's suppression was heard and denied, defendant entered a plea of guilty. (*Michael E.*, *supra*, 230 Cal.App.4th at p. 263.) Defendant appealed, arguing that the trial court erred in denying his motion to suppress video files found in a search of his computer because the warrantless search conducted by the police exceeded the scope of the prior private search. (*Ibid.*)

On appeal, the Government argued that defendant had lost any expectation of privacy when he turned his computer over to the repair person. (*Michael E.*, *supra*, 230 Cal.App.4th at p. 267.)

The First District began by noting that when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities and, if that occurs, the Fourth Amendment does not prohibit governmental use of that information. (*Michael E.*, *supra*, 230 Cal.App.4th at p. 268.) Nevertheless, where the authorities exceed the scope of that private search, they presumptively violate the Fourth Amendment if they act without a warrant. (*Ibid.*, citing *United States v. Jacobsen* (1984) 466 U.S. 109, 115, 117-118.)

The court found that the officers' search of the USB drive clearly exceeded the repair person's prior private search because the repair person had not examined the

materials he placed on the flash drive prior to contacting the police, he had not determined the illicit character of any of the images, and he had been unable to view the materials stored on the computer even after police directed him to open those files. (*Michael E.*, *supra*, 230 Cal.App.4th at p. 275.)

In so finding, the court rejected the trial court's treatment of defendant's hard drive as the functional equivalent of, or analogous to, a "closed container," as that term is used in Fourth Amendment jurisprudence. (*Michael E.*, *supra*, 230 Cal.App.4th at p. 276.) The court thus rejected the trial court's reliance on *U.S. v. Runyan* (5th Cir. 2001) 275 F.3d 449, 464-465, for the proposition that "the police do not exceed the scope of a prior private search when they examine more items within a closed container than did the private searchers." (*Michael E.*, *supra*, 230 Cal.App.4th at pp. 274-276.)

The court noted that, unlike a computer disk, which contains a relatively small amount of data, a computer hard drive ordinarily contains or connects to *all* the information stored in a computer. (*Id.* at p. 276) Relying on the Supreme Court's analysis in *Riley*, *supra*, 134 S.Ct. 2473, the court in *Michael E.* concluded that, because "the search of a computer hard drive implicates at least the same privacy concerns as those implicated by the search of a cell phone, there is no reason to think conventional computers can any more reasonably be characterized as containers than cell phones." (*Michael E.*, *supra*, 230 Cal.App.4th at p. 277, citing *U.S. v. Mitchell* (11th Cir. 2009) 565 F.3d 1347, 1351, 1352 [describing "the hard drive of a computer, which 'is the digital equivalent of its owner's home, [as] capable of holding a universe of private information'"].)

The court therefore held that the trial court erred in denying defendant's suppression motion; the repair person's private search had not frustrated defendant's reasonable expectation of privacy in the materials on his hard drive and the police's subsequent search of defendant's computer exceeded the scope of the private search. (*Michael E.*, *supra*, 230 Cal.App.4th at p. 279.)

c. Ninth Circuit Cases Applying *Riley*

i. *United States v. Camou* (9th Cir. 2014) 773 F.3d 932

In *United States v. Camou* (9th Cir. 2014) 773 F.3d 932, defendant was driving with his girlfriend in the passenger seat, when his truck was stopped by United States Border patrol agents in Westmorland, California. (*Id.* at p. 935.) Agents saw Alejandro Martinez-Ramirez, an undocumented immigrant, lying on the floor behind the truck's front seats, whereupon the agents arrested defendant, his girlfriend, and Martinez-Ramirez, and seized defendant's truck and cell phone. (*Ibid.*) The arrest occurred at about 10:40 p.m. (*Ibid.*)

At 12:00 a.m., an agent searched defendant's cell phone to look for evidence of "known smuggling organizations and information related to the case." (*Camou*, *supra*, 773 F.3d at p. 936.) The agent did not indicate that the search was necessary to prevent

the destruction of evidence or to ensure his or anyone else's safety. (*Ibid.*) After searching the phone's call logs, videos, and photos, the agent saw images of child pornography and notified the FBI. (*Ibid.*)

On August 5, 2009, the FBI executed a federal warrant to search defendant's cell phone for child pornography and found several hundred of such images on the phone. (*Camou*, *supra*, 773 F.3d at p. 936.) Defendant was charged with possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B). (*Ibid.*)

Defendant moved to suppress the images found on his phone, arguing that the warrantless search violated his Fourth Amendment rights. (*Camou*, *supra*, 773 F.3d at p. 936.) The district court denied the suppression motion, finding that the search of the phone was a lawful search incident to arrest and, even if the search was unconstitutional, the good faith and inevitable discovery exceptions to the exclusionary rule were satisfied. (*Ibid.*) Defendant pled guilty to possession of child pornography and appealed the district court's denial of his motion to suppress. (*Ibid.*)

On appeal, the Ninth Circuit determined that the agent's search of the phone was too removed in time from defendant's arrest to be incident to that arrest and, thus, the district court erred in denying the suppression motion. (*Camou*, *supra*, 773 F.3d at pp. 937-938.)

The court rejected the Government's arguments that the search was permissible due to exigent circumstances. (*Camou*, *supra*, 773 F.3d at p. 940.) The Ninth Circuit noted that, despite *Riley*'s assertion of a general warrant requirement for cell phone searches, *Riley* still provided that the exigency exception could "justify a warrantless search of a particular phone" and 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." (*Ibid.*, citing *Riley*, *supra*, 134 S.Ct. at p. 2494.)

In analyzing whether such exigent circumstances existed, the court relied on a hypothetical raised in *Riley* that illustrated an exigent circumstance in the context of a cell phone search—i.e, where circumstances suggest that a phone will be the target of an imminent remote-wipe attempt, and law enforcement cannot prevent remote wiping by disconnecting the phone from the network, the Government could possibly rely on exigent circumstances to search the phone immediately. (*Camou*, *supra*, 773 F.3d at pp. 940-941, citing *Riley*, *supra*, 134 S.Ct. at pp. 2486-2487.) The Ninth Circuit found no such exigent circumstances to exist in defendant's case. (*Id.* at p. 941.)

The court further noted that, even if exigent circumstances had existed to permit the cell phone search, the scope of the search was overbroad because it went beyond contacts and call logs, and included a search of hundreds of photographs and videos. (*Camou*, *supra*, 773 F.3d at p. 941.)

In response to the Government's argument that the search was permissible under the vehicle exception (i.e., officers may search a vehicle and any containers found therein without a warrant, so long as they have probable cause) the Ninth Circuit held that cell phones are not containers for purposes of the vehicle exception. (*Camou*, *supra*, 773 F.3d at p. 942.) In so doing, the court extended the reasoning in *Riley* from the search incident to arrest exception to the vehicle exception. (*Ibid.*) The court provided:

> [T]he privacy intrusion of searching a cell phone without a warrant is of particular concern in the vehicle exception context because the allowable scope of the search is broader than that of an exigency search, or a search incident to arrest. Whereas exigency searches are circumscribed by the specific exigency at hand and searches incident to arrest are limited to areas within the arrestee's immediate control or to evidence relevant to the crime of arrest, vehicle exception searches allow for evidence relevant to criminal activity broadly. If cell phones are considered containers for purposes of the vehicle exception, officers would often be able to sift through all of the data on cell phones found in vehicles because they would not be restrained by any limitations of exigency or relevance to a specific crime.

(*Id.* at p. 943.)

Finally, the court found unavailing the Government's arguments that, even if the warrantless search was unconstitutional, the photographs found should not be suppressed under the inevitable discovery and good faith exceptions to the exclusionary rule. (*Camou*, *supra*, 773 F.3d at pp. 943-945.)

ii. *United States v. Lara* (9th Cir. 2016) 2016 U.S. App. Lexis 3995

The defendant in *United States v. Lara* (9th Cir. 2016) 2016 U.S. App. Lexis 3995 was on felony probation following a conviction for sale and transportation of methamphetamine (Health & Saf. Code §§ 11378 and 11379, subd. (a)). His probation agreement required him to submit to search of "person and property, including any residence, premises, container or vehicle under [his] control . . . with or without a warrant, probable cause, or reasonable suspicion." (*Lara*, *supra*, at p. *3.) As part of his probation agreement, defendant initialed a "Fourth Amendment waiver." (*Id.* at pp. *3-4.) In a sworn declaration, defendant later stated that when he accepted the terms and conditions of probation, he did not believe the search condition would allow his cell phone or data stored on the cell phone to be searched without his consent. (*Id.* at p. *4.)

During a probation search, an officer examined defendant's phone and found text messages containing three photos of a semiautomatic handgun lying on a bed. (*Lara*, *supra*, 2016 U.S. App. Lexis 3995, at pp. *5-6.) Probation officers searched defendant's house and car for the gun, but only found a folding knife, the possession of which violated the terms of defendant's probation. (*Id.* at p. *6.) Defendant was arrested and officers brought the cell phone to a forensics lab. (*Ibid.*)

From examining the GPS data embedded in the photos of the gun, the officers learned that the photos had been taken at the home of defendant's mother. (*Lara*, *supra*, 2016 U.S. App. Lexis 3995, at p. *6.) The officers then searched the home of defendant's mother and found a loaded handgun that resembled the gun in the photographs. (*Id.* at p. *7.) Defendant was charged with being a felon in possession of a firearm and ammunition, in violation of 18 U.S.C. § 922(g)(1). (*Ibid.*)

He moved to suppress the gun and ammunition, arguing that they had been found as a result of the illegal searches of his cell phone, but the district court denied the suppression motion. (*Ibid.*) Defendant pled guilty to the charged offense and appealed the denial of his suppression motion. (*Ibid.*)

The Ninth Circuit first addressed defendant's waiver of his Fourth Amendment rights and determined that, because "a probationer's acceptance of a search term in a probation agreement does not by itself render lawful an otherwise unconstitutional search of a probationer's person or property," the issue was not solely whether defendant accepted the cell phone search as a condition of his probation, but whether the search that he accepted was reasonable. (*Lara*, *supra*, 2016 U.S. App. Lexis 3995, at pp. *8-10.)

In evaluating the reasonableness of the search, the court balanced, "on the one hand, the degree to which [the search] intrudes upon an individual's privacy and, on the other, the degree to which [the search] is needed for the promotion of legitimate governmental interests." (*Lara*, *supra*, 2016 U.S. App. Lexis 3995, at p. *11, citing *United States v. Knights* (2001) 534 U.S. 112, 119.)

To determine the extent to which the search intruded on defendant's privacy, the court noted the following. First, while defendant's privacy interest was lower than someone who had completed probation or who had never been convicted of a crime, it was still greater than the privacy interests of parolees or probationers who had been convicted of particularly serious and violent felonies. (*Lara*, *supra*, 2016 U.S. App. Lexis 3995, at pp. *11-12.)

Second, defendant's cell-phone search condition was not clear because it merely required defendant to submit to search of his "property" and "container[s]"—neither term of which clearly and unambiguously encompassed defendant's cell phone and the information contained therein. (*Id.* at pp. *12-13, citing *Riley*, *supra*, 134 S.Ct. at 2491 [providing that "[t]reating a cell phone as a container whose contents may be searched incident to an arrest" was, at best, "strained"]; *Camou*, *supra*, 773 F.3d at pp. 942-943 [holding that cell phones cannot be searched when officers otherwise have probable cause to search a vehicle and its containers].) Relying on *Riley* and *Camou,* the court held that "it makes no sense to call a cell phone a 'container' for purposes of a probation search." (*Id.* at p. *13.) The court further noted that the term "property" did not unambiguously include cell phone *data*, which is not a physical object that can be possessed, in the manner of the other types of property listed in the probation condition, nor is it necessarily under the defendant's "control," as provided by the search condition. (*Id.* at pp. *13-14.)

Third, the Ninth Circuit emphasized that "[a]lthough *Riley* concerned warrantless searches of cell phones incident to arrest, the Court used sweeping language to describe the importance of cell phone privacy." (*Lara*, *supra*, 2016 U.S. App. Lexis 3995, at p. *14, citing *Riley*, *supra*, 134 S.Ct. at p. 2489.)

The court thus concluded that defendant's privacy interest, albeit somewhat diminished in light of his status as a probationer, was nevertheless substantial "in light of the broad amount of data contained in, or accessible through, his cell phone." (*Lara*, *supra*, 2016 U.S. App. Lexis 3995, at pp. *15-16.)

In weighing the government's interest in the search, the court found the officers' rationale—that the cell phone was searched because defendant had been convicted of a drug crime and "drug traffickers often use cell phones to arrange sales"—unpersuasive. (*Lara*, *supra*, 2016 U.S. App. Lexis 3995, at p. *17.) The court provided:

> Given the ubiquity of cell phones, almost any crime involving more than a single person (and indeed many crimes involving just one person) would entail the use of cell phones, which can be used not only for placing calls and sending text messages, but also for sending emails, looking up directions, and conducting internet searches on various topics. This ubiquity cuts against the government's purported heightened interest in conducting suspicionless searches of the cell phones of probationers with controlled substances convictions.

(*Ibid.*)

On balance, the court therefore found the searches of defendant's cell phone unreasonable. (*Lara*, *supra*, 2016 U.S. App. Lexis 3995, at pp. *17-18.) The court further rejected the Government's argument that a good faith exception to the exclusionary rule should apply based on "binding appellate precedent," and found that pre-*Riley*, the appellate precedent "rather than being binding, [wa]s (at best) unclear." (*Id.* at pp. *18-22.) The court thus reversed the district court's denial of defendant's suppression motion. (*Id.* at p. *22.)

d. Applying *Riley* in Different Fourth Amendment Contexts

A few legal doctrines in Fourth Amendment jurisprudence are still committed to viewing digital data in terms of ill-fitting physical analogues. As such, these doctrines are ripe for reconsideration in light of the Supreme Court's acknowledgment in *Riley* that digital devices and data are different. The Supreme Court's decision in *Riley* may signal its willingness to establish new rules for government searches and seizures as to each of the doctrines and circumstances below.

i. "Third-Party" Doctrine

For example, the "third-party" doctrine establishes that there is no Fourth Amendment interest in information knowingly and voluntarily revealed to "third parties."

(*United States v. Miller* (1976) 425 U.S. 435; *Smith v. Maryland* (1979) 442 U.S. 737.) A "third party" includes any non-governmental institution or entity established by law, such as banks (*Miller*) and phone companies (*Smith*). Under an aggressive reading of the third-party doctrine today, the Fourth Amendment would not guarantee the privacy of any personal data held by any private company, including virtually all records of electronic communications, web browsing activity, and cloud data. (Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine* (2016) 8 J. Nat'l Security L. & Pol'y 247, 264-267.)

Justice Sotomayor has described the third-party doctrine as "ill suited to the digital age" and suggested that it may be necessary to reconsider the premise altogether. (*United States v. Jones* (2012) 132 S.Ct. 945, 957 (Sotomayor, J., concurring).) Today, almost every aspect of online life leaves a "trail of digital breadcrumbs in the form of third-party records." For example, Google keeps a copy of every search it is asked to make and, if possible, links each search to a particular user. Under the third-party doctrine, even semi-private or anonymous messages shared over social media are treated as public. (*Rethinking Privacy*, *supra*, 8 J. Nat'l Security L. & Pol'y at pp. 265-269).

ii. "Plain View" Doctrine

As the search and seizure of stored electronic data has become commonplace in criminal investigations, lower courts have also had to address the application of the "plain view" doctrine to digital searches. (*Get a Warrant*, *supra*, 10 Duke J. Const. Law & Pub. Pol'y at p. 114, citing Kerr, *Searches and Seizures in a Digital World* (2005) 119 Harv. L. Rev. 531 [discussing the application of the plain view doctrine to searches of various digital mediums].) The Supreme Court held in *Arizona v. Hicks* (1987) 480 U.S. 321 and *Horton v. California* (1990) 496 U.S. 128 that "[i]f an article is already in plain view, neither its observation nor its seizure would involve any invasion of privacy." (*Id.* at p. 133, citing *Hicks*, *supra*, at p. 325.) When applied to seizures of digital data, however, questions arise as to what data is in plain view once a computer directory is examined by government agents. (See *U.S. v. Comprehensive Drug Testing (CDT)* (9th Cir. 2010) 621 F.3d 1162 (en banc).

iii. Cell Phone Location Data

Additionally, *Riley* may affect the state of Fourth Amendment protection for cell phone location data. In *Jones*, *supra*, 132 S.Ct. at p. 949, the Supreme Court held that "the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search'" under the Fourth Amendment." But the majority opinion in *Jones* ruled on the narrower grounds that the government's physical occupation of the defendant's "private property for the purpose of obtaining information" constituted a search, regardless of whether the defendant had a "reasonable expectation of privacy" in his location information. (*Id.* at p. 950.)

Although the Court in *Jones* did not directly answer whether the collection of location data without the use of a physical tracking device is a "search" under the Fourth

Amendment, two concurring opinions—one by Justice Sotomayor and another by Justice Alito, joined by three other justices—reasoned that the long-term monitoring of an individual's location would violate a reasonable expectation of privacy. (*Id.* at p. 956 (Sotomayor, J., concurring); *id.* at p. 964 (Alito, J., concurring). Although the state of Fourth Amendment protection for location data is uncertain post-*Jones*, the Court in *Riley* specifically addressed the sensitivity of location data in noting, "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." (*Riley*, *supra*, 134 S.Ct. at p. 2495, citing *Jones*, *supra*, 132 S.Ct. at p. 955.) Given the Court's findings on the significant privacy interests at stake in location data, it would be difficult for a lower court to conclude that an individual has "no reasonable expectation of privacy" in such sensitive data. (*Get a Warrant*, *supra*, 10 Duke J. Const. Law & Pub. Pol'y at pp. 109-111.)

II. California Electronic Communications Privacy Act (CalECPA, SB 178)

a. Synopsis of CalECPA

The California Electronic Communications Privacy Act (Pen. Code, Ch. 3.6, added by Stats. 2015, Ch. 651) was approved by the Governor on October 8, 2015, after it passed both chambers of the California legislature with 2/3 support. (Electronic Frontier Foundation, *California's Electronic Communications Privacy Act*, <https://www.eff.org/cases/californias-electronic-communications-privacy-act-calecpa> [as of March 27, 2016].) The Act took effect on January 1, 2016. (§ 1546 et seq.)

CalEPCA has been touted as the most comprehensive digital privacy law in the nation. It prohibits a California governmental entity from compelling the production of, or access to, electronic communication information without a search warrant, wiretap order, order for electronic reader records, or subpoena issued pursuant to specified conditions, except for certain defined emergency situations. (Daniels, *California Updates Privacy Rights with the Electronic Communications Privacy Act* (Jan. 17, 2015) JDSupra < http://www.jdsupra.com/legalnews/california-updates-privacy-rights-with-55097/> [as of March 27, 2016].)

In other words, it requires *all* California state and local law enforcement agencies to obtain a search warrant or wiretap order before they can access any electronic communication information. The law defines "electronic communication information" in the broadest terms possible, to include emails, digital documents, text messages, location information, and any digital information stored in the cloud. The law protects all aspects of electronic communication information, not just its content, but also metadata information relating to the sender, recipient, format, time, date, and location of the communications, including IP addresses. (Daniels, *California Updates Privacy Rights*, *supra*.)

CalEPCA also limits the ability to California law enforcement to obtain information directly from a smartphone or similar device, or to track those devices. Law

enforcement must either obtain a warrant, or get the consent of the person possessing the electronic device, before getting any such information. (Daniels, *California Updates Privacy Rights, supra.*)

Any electronic evidence obtained in violation of CalEPCA will be inadmissible in a criminal, civil, or administrative proceeding or for use in an affidavit to obtain a search warrant or court order. (See § 1546.4.) Furthermore, CalEPCA requires government entities that receive electronic communication without a warrant to delete the information within 90 days. (Daniels, *California Updates Privacy Rights, supra.*)

If a warrant is issued to a third party that is in possession of a person's electronic communications, such as Facebook or Google, CalEPCA requires law enforcement to contemporaneously inform the user that there has been a request for their electronic information and specify the nature of the government investigation under which the information is sought. (Daniels, *California Updates Privacy Rights, supra.*)

There are, nevertheless, exceptions to the warrant requirement. If an owner of a device gives a law enforcement official permission to access data on their electronic device, or if a government entity believes an electronic device has been lost or stolen, it can access it to try to identify, verify, or contact the owner. There is also an emergency exception. If a law enforcement official believes that an emergency involving "danger of death or serious physical injury to any person" requires access to the electronic device information, then he or she can access the information. The government official will still, however, have to file for a warrant within three days of obtaining the data. (Daniels, *California Updates Privacy Rights, supra.*)

III. Electronic Searches & Digital Privacy in Probation Conditions

a. Synopses of Recent Opinions

i. *People v. Pirali* (2013) 217 Cal.App.4th 1341

In *People v. Pirali* (2013) 217 Cal.App.4th 1341, defendant pleaded no contest to felony possession of child porn and the trial court imposed conditions of probation that included, *inter alia*, the following: "You're not to enter any social networking sites, nor post any ads, either electronic or written, unless approved by a probation officer"; "You're to report all personal e-mail addresses used and shall report Web sites and passwords to the probation officer within five days"; "You are not to have access to the Internet or any other on-line service through use of your computer or other electronic device at any location without prior approval of the probation officer. And shall not possess or use any data encryption technique program." (*Id.* at p. 1344.) Defendant challenged the probation condition restricting his Internet access on grounds of vagueness and overbreadth. (*Id.* at pp. 1345-1346.)

In analyzing the conditions for overbreadth, the Sixth District began by noting that "access to computers and the Internet have been recognized by courts as increasingly

important" and that computers and the Internet now "'comprise[] the "backbone" of American academic, governmental, and economic information systems."'" (*Pirali*, *supra*, 217 Cal.App.4th at p. 1348, citing *U.S. v. Peterson* (2d Cir. 2001) 248 F.3d 79, 83 ["Computers and Internet access have become virtually indispensable in the modern world of communications and information gathering."]; *In re Stevens* (2004) 119 Cal.App.4th 1228, 1234.) Accordingly, the court found that certain restrictions on access to the Internet necessarily curtail First Amendment rights and, thus, that probation conditions restricting or prohibiting the use of a computer, or restricting or prohibiting access to the Internet, must closely tailor those limitations to the purpose of the condition to avoid being invalidated as unconstitutionally overbroad. (*Pirali*, *supra*, at p. 1348, citing *Sheena K.*, *supra*, 40 Cal.4th at p. 890; *Stevens*, *supra*, at p. 1237.)

Nevertheless, the Sixth District found that the probation condition in *Pirali* was not constitutionally overbroad because defendant was "not faced with a blanket prohibition" but instead "clearly grant[ed] defendant the ability to access the Internet on his computer and other electronic devices so long as he obtains prior permission from his parole officer. " (*Pirali*, *supra*, 217 Cal.Appl.4th at p. 1350.) The court further noted that defendant "may still use the Internet and a computer while at home, or at his place of employment," and that he "may also still continue to access and use the Internet for e-mail, and other methods of online communication, subject to prior approval by his probation officer." (*Id.* at p. 1350.)

In analyzing the probation conditions for vagueness, the Sixth District found that, in the absence of an express knowledge requirement, defendant could "unwittingly violate the condition as there are situations in which he may not know he has access to or has accessed the Internet." (*Pirali*, *supra*, 217 Cal.Appl.4th at p. 1350.) Thus, the court modified the probation condition to add a requirement that defendant must *knowingly* have access to the Internet. (*Id.* at p. 1351.) The court further found that the phrase "other electronic devices" was not unconstitutionally vague, when modified to include an express knowledge requirement, even though "use of a smartphone, Kindle, or even a swipe of [defendant's] credit card may inadvertently put him on the Internet." (*Id.* at pp. 1351-1352.)

ii. *In re Erica J.* (2015) 240 Cal.App.4th 907

In *In re Erica J.* (2015) 240 Cal.App.4th 907, the defendant challenged the condition which required her to provide her passwords and to submit her electronic devices to search as unreasonable under *People v. Lent* (1975) 15 Cal.3d 481. (*Erica J.*, *supra*, at p. 911.) The appellate court found the search condition bore no relationship to the underlying offense of possession of Ecstasy, because there was no indication in the record that she had used of any devices or social media to purchase illegal substances. (*Id.* at p. 912 - 913.) The court found the second prong of *Lent*, that the conduct itself – the use of electronic devices and social media - was not itself criminal. (*Id.* at p. 913.) Last, the electronic search condition was not reasonably related to future criminal conduct. (*Ibid.*) Because there was nothing in the record "regarding either the current offense or [defendant's] social history that connects her use of electronic devices or

social media to illegal drugs...[and] the record is wholly silent about [defendant's] usage of electronic devices or social media, ... there is nothing in [defendant's] past or current offenses or [her] personal history that demonstrates a predisposition" to utilize electronic devices or social media in connection with criminal activity, there is no reason to believe the current restriction will serve the rehabilitative function of precluding the [defendant] from any future criminal acts. [Citation omitted.]" (*Ibid.*)

iii. *In re Malik J.* (2015) 240 Cal.App.4th 896

In *In re Malik J.* (2015) 240 Cal.App.4th 896, the 17-year old defendant and one or two companions assaulted and robbed three women near the MacArthur Street BART, and one of the robberies involved an iPhone. (*Id.* at pp. 899-900.) The juvenile court imposed probation conditions requiring defendant and his family to "provide all passwords to any electronic devices including cell phones, computers and notepads within your custody and control" and to "provide any passwords to any social media sites . . . and submit those [s]ites to any peace officer with or without a warrant." (*Id.* at p. 900.)

The First District found the search conditions overbroad. (*Malik J.*, *supra*, 240 Cal.App.4th at p. 902.) Citing *Riley*, *supra*, 135 S.Ct. 2473, the court emphasized the significant privacy interests threatened by unfettered searches of electronic communications, remotely stored information, and social networking sites, for both defendant and "third parties who are not otherwise subject to search or court supervision." (*Id.* at pp. 902-903.) The court thus counseled narrowing the conditions as follows:

> Officers must be able to determine ownership of any devices in a probationer's custody or within his or her control, and search them if they belong to the probationer or if officers have a good faith belief that he or she is a permissive user. But in performing such searches, officers must show due regard for information that may be beyond a probationer's custody or control or implicate the privacy rights of the probationer or third parties. Officers should not be allowed to conduct a forensic examination of the device utilizing specialized equipment that would allow them to retrieve deleted information that is not readily accessible to users of the device without such equipment. They should also first disable the device from any internet or cellular connection. These measures will limit a search to information that is stored on the device and accessible to the probationer, and thus in the probationer's possession and subject to his or her control.

(*Id.* at pp. 903-904.)

The court rejected, however, defendant's argument that it was unreasonable to require him to provide passwords for electronics found in his custody and control "because officers can identify a phone's legal owner by using identifying numbers and codes found on the devices." (*Malik J.*, *supra*, 240 Cal.App.4th at p. 904.)

The court further rejected defendant's contention that the phrase "any electronic devices" in the search condition was unconstitutionally vague and, instead, found it "reasonably clear that the condition applies to similar electronic devices within Malik's custody and control that might be stolen property and not, as Malik conjectures, to authorize a search of his Kindle to see what books he is reading or require him to turn over his ATM password." (*Malik J.*, *supra*, 240 Cal.App.4th at pp. 904-905.)

Finally, the court found the probation condition "indisputably unconstitutional so far as it could be read to require individuals other than Malik to submit to warrantless searches of their electronic devices or turn over their passwords to police on demand" and, thus, ordered any reference to defendant's family stricken. (*Malik J.*, *supra*, 240 Cal.App.4th at p. 906.)

iv. *In re Ricardo P.* (2015) 241 Cal.App.4th 676 & *In re Alejandro R.* (2015) 243 Cal.App.4th 556: Both Superseded by Grant of Review

The court in *In re Ricardo P.* (2015) 241 Cal.App.4th 676, found a probation condition, which required the defendant to submit to a search of his electronics and to provide passwords, did not meet the third prong of *Lent* because it was "reasonably related to preventing future criminality" and, thus, the condition was not unreasonable. (*Id.* at pp. 685-687.)

There, after the defendant admitted to two felony counts of first degree burglary under Penal Code sections 459 and 460, subdivision (a), the juvenile court ordered several drug-related conditions. (*Ricardo P.*, *supra*, 241 Cal.App.4th at pp. 680-681.) The defendant argued that one of the search conditions, which required him to submit to an electronic search and to provide his passwords, was not reasonably related to future criminality because there was no evidence he used any electronics to discuss his past marijuana use. (*Id.* at p. 685.) Although there were no allegations of illegal substance abuse, the defendant told probation that he had smoked marijuana in the past. (*Id.* at pp. 681, 689.) The court found that "the electronics search condition is reasonably related to enabling the effective supervision of [defendant's] compliance with his other probation conditions" and that it was within the court's discretion to impose this condition to address the concern that the defendant might use his electronics to communicate about drugs. (*Id.* at p. 686.)

Review was granted in *Ricardo P.* on February 17, 2016, so the Court of Appeal opinion has been depublished.

In *In re Alejandro R.* (2015) 243 Cal.App.4th 556, a juvenile admitted to being an accessory to illegal drug sales and, as a condition of probation, the court required him to submit to the warrantless search of his "electronics . . . and passwords." (*Id.* at p. 560.) In explaining the rationale for the probation condition, the court provided, "As in this case with drugs, I find it's very important [and]the best way of supervising individuals like yourself [who] have drug cases, that we check your electronics, because that's where

you buy and sell and very often boast with photos about your drug usage and drug paraphernalia." (*Id.* at p. 561.) Following the court's reasoning in *In re Ricardo P.* (2015) 241 Cal.App.4th 676, the appellate court interpreted the electronic search condition to not only include electronic devices and the data contained on them, but also "electronic accounts, such as social media accounts, that, while not stored on electronic devices, can be accessed through them." (*In re Alejandro R.*, *supra*, 243 Cal.App.4th at p. 563.)

As to the first *Lent* element, the courts in both *In re Alejandro R.* (2015) 243 Cal.App.4th 556 and *In re Ricardo P.* (2015) 241 Cal.App.4th 676 determined that nothing in the records permitted an inference that the defendants had used electronic devices or social media in the commission of their crimes. (See *In re Alejandro R.*, *supra*, at p. 564; *In re Ricardo P.*, *supra*, at pp. 684-685.) As to the second *Lent* element, the courts in both *Alejandro R.* and *Ricardo P.* assumed that the use of electronic devices is not illegal. (*Alejandro R.*, *supra*, 243 Cal.App.4th at p. 564; *Ricardo P.*, *supra*, 241 Cal.App.4th at p. 685.)

As to the third prong of *Lent*, however, the courts in *Alejandro R.* and *Ricardo P.* determined that the conditions permitting warrantless searches of the defendants' electronic devices and social media accounts were reasonably related to future criminality. (*Alejandro R.*, *supra*, 243 Cal.App.4th at p. 564; *Ricardo P.*, *supra*, 241 Cal.App.4th at p. 686.) In doing so, the courts relied on *People v. Olguin* (2008) 45 Cal.4th 375, in which the Supreme Court considered the validity of a probation condition requiring an adult probationer to inform the probation officer of the presence of pets in his residence. The *Olguin* court noted that it was important for a probation officer conducting a search of the probationer's residence to know whether he or she would encounter pets at the residence. The court concluded that a probation condition "that enables a probation officer to supervise his or her charges effectively is . . . 'reasonably related to future criminality.'" (*Id.* at pp. 380-381.)

Based on the reasoning in *Olguin*, the court in *Ricardo P.* determined that, because an electronics search condition is "reasonably related to enabling the effective supervision of [the appellant's] compliance with his other probation conditions," it was valid. (*Ricardo P.*, *supra*, 241 Cal.App.4th at p. 686.)

Somewhat relatedly, the court in *Alejandro R.* found that, "[a]lthough there was no evidence [the defendant] used electronics in connection with [his] violations, that does not mean [his] electronic devices and social media use are irrelevant to the rehabilitative and reformative purpose of the juvenile court." (*In re Alejandro R.*, *supra*, 243 Cal.App.4th at p. 567.) The court found that, because "cell phones and social media are used to further, and even to celebrate, juvenile drug use," and the trial court "imposed the electronics search condition in an attempt to ensure [the defendant] did not use electronics and social media for such purposes," given the deferential standard of review, the appellate court was "unwilling to hold that the condition was so unrelated to the juvenile court's goal of preventing appellant from selling and consuming illegal drugs as to constitute a manifest abuse of discretion." (*Ibid.*)

The First District in *Alejandro R.* then concluded that the conditions, as imposed, were constitutionally overbroad. (*In re Alejandro R.*, *supra*, 243 Cal.App.4th at p. 560.) The court limited the scope of the permissible searches to "programs used for interpersonal communication" that might reveal drug activity. (*Id.* at p. 568.)

Review was granted in *Alejandro R.* on March 9, 2016, so the Court of Appeal opinion has been depublished.

v. *In re J.B.* (2015) 242 Cal.App.4th 749

In *In re J.B.* (2015) 242 Cal.App.4th 749, the juvenile defendant admitted to committing a petty theft from Sears. (*Id.* at p. 752.) As a condition of probation, the court required him to submit to a search of "[his] electronics including [his] passwords." (*Ibid.*) The court explained the necessity of the probation condition by underscoring defendant's possible communication with his co-participant in the petty theft; his potential to use the Internet to purchase, sell, or use drugs (the minor had admitted to using marijuana); and a report that defendant had been playing with his cell phone during an interview with his mother and a probation officer. (*Id.* at p. 753.)

On appeal, the First District found the probation condition invalid under *Lent*, *supra*, 15 Cal.3d at p. 486 because: (1) the electronic search condition had no relationship to the crime of petty theft or to the specific offense the minor admitted committing and there was no evidence in the record that the minor used email, texting, or social networking Web sites to facilitate his offense; (2) it was "beyond dispute that the use of electronic devices and of social media is not itself criminal"; and (3) much like the circumstances of *Erica R.*, *supra*, 240 Cal.App.4th at p. 913, because there was nothing in the minor's past or current offenses or his personal history that demonstrated a predisposition to utilize electronic devices or social media in connection with criminal activity, there was no reason to believe the probation condition would serve the rehabilitative function of precluding the minor from any future criminal acts. (*J.B.*, *supra*, 242 Cal.App.4th at pp. 754-755.) Finally, the court noted that the electronic search condition was not properly tailored to fit the circumstances of the case and the minor, and was, therefore, invalid under *Lent*.

The court further found the requirement that defendant submit his electronic devices for search and provide his probation officer with his electronic passwords constitutionally overbroad and struck the condition. (*J.B.*, *supra*, 242 Cal.App.4th at pp. 756-757.)

In so doing, the court disagreed with the opinions of *Ricardo P.*, *supra*, 241 Cal.App.4th 676 and *Patrick F.*, *supra*, 242 Cal.App.4th 104, insofar as those opinions relied on *Olguin*, *supra*, 45 Cal.4th 375 to justify probation conditions facilitating general supervision of a ward's activities where the conditions required or forbade noncriminal conduct bearing no relation to the minor's offense, that was not reasonably related to potential future criminality as demonstrated by the minor's history and prior misconduct. (*J.B.*, *supra*, 242 Cal.App.4th at p. 757.) The court determined that such broad probation

conditions could not be squared with the limitations imposed by *Lent*, *supra*, 15 Cal.3d at p. 486 and, in some cases, could exceed constitutional limitations. (*J.B.*, *supra*, 242 Cal.App.4th at pp. 757-758.)

The court questioned the ability of the juvenile court to articulate a "narrower range of electronic information" to be searched that would preserve the minor's legitimate privacy interests. (*J.B.*, *supra*, 242 Cal.App.4th at p. 758.) In support of its skepticism, the court cited the language in *Riley*, *supra*, 134 S.Ct. at p. 2492 providing that "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 . . . 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." (*J.B.*, *supra*, 242 Cal.App.4th at p. 759.)

Finally, while the court agreed with the observations in *Ricardo P.* and *Patrick F.* that the minor had no standing to raise the privacy interests of third parties, the court found "no justification for the court to authorize probation officers to invade the privacy of other innocent parties who participate in the same social media networks as the minor." (*J.B.*, *supra*, 242 Cal.App.4th at p. 759.)

vi. *People v. Navarro* (2016) 244 Cal.App.4th 1294

In *People v. Navarro* (2016) 244 Cal.App.4th 1294, the Fourth District Court of Appeal considered a special condition of parole that restricted defendant's use of "an electronic bulletin board system, [I]nternet relay chat channel, instant messaging, newsgroup, usergroup, peer to peer; i.e., Napster, Gnutella, Freenet, etc." and "any site-base; i.e., Hotmail, Gmail, or Yahoo e-mail, etc., which allows the user to have the ability to surf the [I]nternet undetected." (*Id.* at p. 1297.) Defendant was also subject to four other conditions restricting his computer and electronic media use, including a condition that prohibited him from using a computer for sexual activity, i.e., "'chat[ting],'" e-mail, usergroups, newsgroups, and list servers. (*Ibid.*) The 19-year old Navarro had pleaded guilty to attempted kidnapping (§§ 664, 207, sudb. (a)), after grabbing a 13-year old's arms at a bus stop and threatening to rape her. (*Id.* at p. 1296.)

In analyzing defendant's parole conditions under *In re Stevens* (2004) 119 Cal.App.4th 1228, the Fourth District determined that, because Navarro had not used a computer during the underlying offense, the conditions restricting his computer usage were not directly related to the crime of conviction. (*Navarro*, *supra*, 244 Cal.App.4th at p. 1299.) Nevertheless, the court found the parole conditions reasonably related to preventing future criminality. (*Ibid.*) The court found that the trial court had not abused its discretion by imposing a parole condition that sought to deter Navarro from using Internet technologies to "prey on young victims," when his behavior during the underlying offense exhibited "sexual deviancy and sex offender profile behavioral characteristics" that implicated a "type of predatory behavior." (*Id.* at pp. 1299-1300.) The court further pointed to Navarro's failure to abide by the parole conditions related to

Internet use to bolster its conclusion that the parole condition was "reasonably related to deterring future criminal conduct," and was, therefore, valid. (*Id.* at p. 1300.)

The court noted multiple ways of interpreting the parole condition. (*Navarro, supra*, 244 Cal.App.4th at pp. 1301-1302.) First, it could prohibit the use of any e-mail or Internet browser that allows Internet searching in "private" mode. (*Id.* at p. 1301.) Second, it could prohibit the use of instant messaging, peer-to-peer communications, or bulletin boards that allow the user to surf the Internet undetected. (*Ibid.*) And third, it could prohibit parolees from visiting any platform that allows them to browse the Internet undetected by listing types of platforms prohibited (electronic bulletin board systems, Internet relay chat channels, instant messaging, newsgroup, usergroup, and peer-to-peer) and specific platforms prohibited (Napster, Gnutella, Freenet, Hotmail, Gmail, and Yahoo e-mail). (*Ibid.*)

The court further found that the phrase "surf the Internet undetected" made it unclear whether it applied to parolees surfing the Internet undetected by parole authorities, or to parolees interacting with others on the Internet without revealing their identities. (*Navarro, supra*, 244 Cal.App.4th at pp. 1301-1302.) Additionally, the court determined that the inclusion of specific email platforms in the parole condition "causes confusion about whether the Special Condition prohibits the parolee from using e-mail altogether, which would unnecessarily infringe on his right to communicate with family/friends or find/keep employment, or whether the parolee can use e-mail, just not to browse the Internet undetected." (*Id.* at p. 1302.) Finding that the parole condition was subject to "many interpretations and resulting confusion," the Fourth District concluded that it was unconstitutionally vague as written. (*Navarro, supra*, 244 Cal.App.4th at p. 1302.)

vii. *People v. Appleton* (2016) 245 Cal.App.4th 717

In *People v. Appleton* (2016) 245 Cal.App.4th 717, the defendant pleaded no contest to false imprisonment by means of deceit, based on an incident in which defendant and two other men forced John Doe to orally copulate them. (*Id.* at p. 719.) Defendant had met Doe through Grindr, a social media application for smartphones, and the two had had a consensual relationship lasting several months before the underlying incident. (*Id.* at pp. 719-720.)

As a condition of probation, the defendant was required to: (1) subject his computers and electronic devices to search for material prohibited by law; and (2) not clean or delete his Internet browsing activity, and maintain his history for a minimum for four weeks. (*Appleton, supra*, 245 Cal.App.4th at p. 721.) The conditions were imposed over defendant's objections; defendant had argued that the conditions violated his rights under the First, Fourth, Fifth, and Fourteenth Amendments, and that they were vague, overbroad, and unreasonable under *Lent, supra*, 15 Cal.3d 481. (*Appleton, supra*, at p. 721.)

On appeal, as to defendant's *Lent* argument, the Sixth District agreed that "the nexus between the offense and the probation condition [wa]s somewhat attenuated," but found that, due to the deferential standard of review required in the *Lent* analysis, the trial court had not abused its discretion in finding that "either social media or some kind of computer software" had been involved in the offense. (*Appleton*, *supra*, 245 Cal.App.4th at p. 724.) Because all three *Lent* factors must be met before a probation condition can be held invalid, and the court found the first *Lent* factor was not met, the court thus concluded that the challenged conditions were valid under *Lent*. (*Id.* at p. 724.)

The Sixth District nevertheless determined that the electronic search condition was overbroad, in violation of the Fourth Amendment and defendant's rights of privacy. (*Appleton*, *supra*, 245 Cal.App.4th at pp. 724-727.) In so finding, the court noted that, although defendant had ultimately agreed to his probation search conditions, he had not forfeited his claims challenging the computer search condition because he had placed his objections on the record at a hearing scheduled to consider his claims. (*Id.* at p. 725.)

The court additionally determined that the electronic search condition swept more broadly than the standard condition allowing for searches of probationers' persons, vehicles, and homes, because a search of electronic devices could expose a large volume of documents or data, much of which could have nothing to do with illegal activity, and could include, for example, medical records, financial records, personal diaries, and intimate correspondence with family and friends. (*Appleton*, *supra*, 245 Cal.App.4th at p. 725.) The court further found that the trial court's attempt to limit the scope of the search to "material prohibited by law" constituted "no limitation at all" because "[n]othing in the record evidence[d] any technology that would allow a forensic technician to determine whether a computer file or document contain[ed] unlawful material without first examining its contents" and, thus, a technician would first have to view a file, compromising defendant's privacy, before determining whether it constituted prohibited material. (*Id.* at pp. 725-726.) Like the electronic search conditions considered in the recent First District cases concerning juveniles (e.g., *In re Mark C.* (2016) 244 Cal.App.4th 520; *J.B.*, *supra*, 242 Cal.App.4th 749; *Erica R.*, *supra*, 240 Cal.App.4th 907; *Malik J.*, *supra*, 240 Cal.App.4th 896), the Sixth District found that the electronic search condition allowed for searches of vast amounts of personal information unrelated to defendant's criminal conduct or his potential for future criminality. (*Appleton*, *supra*, *Appleton*, *supra*, 245 Cal.App.4th at pp. 726-727.)

The court noted that the state's interest in monitoring whether defendant was using social media to contact minors for unlawful purposes could be met through narrower means. (*Appleton*, *supra*, 245 Cal.App.4th at p. 727.) For example, defendant could provide his social media accounts and passwords to his probation officer for monitoring, or the court could restrict defendant's use of, or access to, social media sites and applications without prior approval of his probation officer. (*Ibid.*) Finding the electronic search condition overbroad, the court struck the condition and remanded for the trial court to consider fashioning a more narrowly tailored condition. (*Ibid.*)

As to the probation condition that required defendant to maintain his browser history, the Sixth District determined that, for the same reasons provided regarding the first considered probation condition, the condition was not invalid under *Lent*. (*Appleton*, *supra*, 245 Cal.App.4th at p. 728.) The court further found that the condition would be necessary to enforce any condition imposed by the trial court on remand that would allow a probation officer to monitor or restrict defendant's use of social media. (*Ibid.*) Finally, the court found that no scienter requirement was necessary because there was "nothing inherently vague or ambiguous about requiring defendant not to delete his browser history." (*Ibid.*)

viii. *In re A.S.* (2016) 245 Cal.App.4th 758

In *In re A.S.* (2016) 245 Cal.App.4th 758, the 17-year old defendant admitted committing a misdemeanor assault by means likely to produce great bodily injury (§ 245, subd. (a)(4)) against her mother. (*A.S.*, *supra*, 245 Cal.App.4th at pp. 762-763.)

Based on a troubling probation report and mental health evaluation of the minor, the court imposed, amongst other conditions, a probation condition subjecting the minor to a "'four way search clause' that included her electronic devices and passwords. (*A.S.*, *supra*, 245 Cal.App.4th at p. 765.) Defense counsel opposed the condition but did not argue "how the electronic search clause might impact appellant's privacy rights in particular, nor did it suggest how the clause might be made more specific while still meeting the concerns of the juvenile court." (*Ibid.*) After a hearing on defendant's motion, the court imposed the electronic search condition. (*Id.* at p. 766.)

On appeal, after noting the significant psychological and behavioral issues facing defendant, the First District determined that the electronic search condition was valid under the *Lent* test because "[i]n this case, appellant's history and circumstances mandate a degree of supervision which reasonably connects the electronic search condition to the prevention of future criminality." (*A.S.*, *supra*, 245 Cal.App.4th at p. 770.) The court further found that, like the circumstances of *Olguin*, *supra*, 45 Cal.4th at p. 378, "the electronic search condition is reasonably related to deterring future criminality because it facilitates the type and level of supervision of appellant which is absolutely necessary for her to succeed on probation." (*A.S.*, *supra*, 245 Cal.App.4th at p. 771.) Finally, the court found that, like the defendant in *People v. Ebertowski* (2014) 228 Cal.App.4th 1170, 1177, the electronic search condition imposed against the minor would be "the best if not the only way to safely place her with her sister without posing an extreme risk to the safety of herself, her mother and the public." (*A.S.*, *supra*, 245 Cal.App.4th at p. 771.)

The court rejected defendant's overbreadth argument, noting that no arguments were raised below to create a record "supporting the supposition that 17-year-old appellant has applications relating to banking, health care, or educational Web sites or accounts," nor did the record "offer any information as to how appellant uses electronic devices and how the search clause might infringe on her daily privacy." (*A.S.*, *supra*, 245 Cal.App.4th at p. 773.) The court further noted that, if defendant could "articulate specific concerns as to how the electronic search clause actually impacts her privacy

adversely, that matter may be brought to the attention of the juvenile court in a motion to modify the terms of appellant's probation." (*Id.* at p. 774.)

Finally, the court rejected appellate counsel's argument that the electronic search condition permitted intrusion on the privacy of third parties in violation of section 632, and determined that: (1) the argument was forfeited because it was not raised in the trial court; and (2) defendant lacked standing to raise the issue. (*A.S.*, *supra*, 245 Cal.App.4th at p. 775.)

b. Consider Raising These Potential Arguments

i. Infringements on the Rights of Third Parties

Where probation conditions allow for searches outside of defendant's immediate control (e.g., computers or electronic devices he may leave at work or with a friend or relative, or computers or devices he might share with coworkers, family members, or roommates), those conditions may infringe on the privacy interests of third parties.

Some opinions have noted that a defendant lacks standing to raise a claim on behalf of a third party. (See, e.g., *A.S.*, *supra*, 245 Cal.App.4th at p. 775; *Ricardo P.*, *supra*, 241 Cal.App.4th at p. 683, superseded by grant of review; *In re Patrick F.* (2015) 242 Cal.App.4th 104, 114, superseded by grant of review.)

Nevertheless, the impact of probation conditions on the privacy interests of third parties has been considered in appellate courts' evaluation of the reasonableness of the probation condition and constitutional overbreadth. (See, e.g., *In re Malik J.* (2015) 240 Cal.App.4th 896, 903, 906 ["Remotely stored information may also implicate the privacy interests of third parties who are not otherwise subject to search or court supervision. . . . [T]he probation condition is indisputably unconstitutional so far as it could be read to require individuals other than [defendant] to submit to warrantless searches of their electronic devices to turn over their passwords to police on demand."]; *In re J.B.* (2015) 242 Cal.App.4th 749, 759 ["[W]hile we agree with the courts' observation in *Ricardo P.* and *Patrick F.* that the minor has no standing to raise the privacy interest of third parties, that is no justification for the court to authorize probation officers to invade the privacy of other innocent parties who participate in the same social media networks as the minor."]; see also *Members of City Council v. Taxpayers for Vincent* (1984) 466 U.S. 789, 801 ["In short, there must be a realistic danger that the statute itself will significantly compromise recognized First Amendment protections of parties not before the Court for it to be facially challenged on overbreadth grounds."].)

Finally, the case law regarding probation searches provides some analogous support for a third party argument. As a general rule, individuals living with probationers subject to search conditions forfeit their Fourth Amendment rights with respect to common areas where the probationer might store property. (*People v. Robles* (2000) 23 Cal.4th 789, 795-796.) However, warrantless searches of the non-probationer's property are not permitted when the area searched is clearly not a common area. (*People v. Romeo*

(2015) 240 Cal.App.4th 931, 935 [search condition for probationers living in a house did not allow for warrantless search of attached garage where a non-probationer resided].) As the *Romeo* court noted, non-probationers are "entitled to demand adherence to the proper scope of [the probationer's] search conditions, despite the usual rule prohibiting the assertion of someone else's Fourth Amendment rights in search and seizure cases. [Citation]." (*Id.* at p. 953.) By parity of reasoning, the same reasoning applies to broad electronic searches. A third party should be entitled to the strict construction of a probationer's electronic search condition in order to protect her own privacy.

ii. Fifth Amendment

The Fifth Amendment to the United States Constitution, which applies to the states by virtue of the Fourteenth Amendment, provides that no person may be compelled to be a witness against himself or herself. (U.S. Const., 5th Amend.; *Maryland v. Shatzer* (2010) 559 U.S. 98, 103 [175 L. Ed. 2d 1045, 1052, 130 S.Ct. 1213]; *People v. Linton* (2013) 56 Cal.4th 1146, 1170-1171.)

An individual must show four things to fall within the ambit of the Fifth Amendment; the information sought must be: (1) incriminating; (2) personal to the defendant; (3) obtained by compulsion; and (4) testimonial or communicative in nature. (*Izazaga v. Superior Court* (1991) 54 Cal.3d 356, 366.)

In *Fisher v. United States* (1976) 425 U.S. 391, the Supreme Court indicated that one's act of producing documents could qualify as testimonial if conceding the existence, possession and control, and authenticity of the documents tended to incriminate that person. Twenty-four years later, in *United States v. Hubbell* (2000) 530 U.S. 27, the Supreme Court reaffirmed that the production of documents is testimonial for purposes of the Fifth Amendment where the Government had no knowledge of the existence of documents, other than a suspicion that such documents likely existed and, if they did exist, that they would fall within the broad categories requested. (*Id.* at pp. 44-45.)

In analyzing whether a condition requires an implicit communicative act, be especially wary of requirements that defendants provide all passwords to email and social media accounts, especially when such conditions are coupled with requirements that the defendant maintain his or his Internet browsing history. Such conditions may be tantamount to mandating testimony by defendant of his or her knowledge of the existence and location of certain personal email and social media accounts, as well as his or her possession, control, and access to those accounts. In other words, the required disclosures assert that the defendant is a member of the online communities and social networks for which he maintains an account. Without these probation conditions, the Government has no knowledge of the Internet communities to which the defendant might belong. (See Murphy, *Social Media Evidence in Government Investigations and Criminal Proceedings: A Frontier of New Legal Issues* (2013) 19 Rich. J.L. & Tech. 11 ["There are hundreds of social networking websites with each catering to a different demographic and providing a different type of content."].)

That is, requiring a defendant's disclosure of the passwords and/or Internet browsing history to reveal and gain access to accounts of which the Government would otherwise have no knowledge, requires the defendant to "disclose the contents of his own mind" (*Curcio v. United States* (1957) 354 U.S. 118, 128), and thus, to provide a testimonial or communicative act.

A defendant's production of those testimonial or communicative acts, in the way of producing passwords and/or Internet browsing history, could well be accompanied by implied factual statements that could prove to be incriminatory. (See *Hubbell*, *supra*, 530 U.S. at p. 43; see also *In re Grand Jury Subpoena Duces Tecum* (11th Cir. 2012) 670 F.3d 1335, 1346-1349 [relying on this reading of *Fisher* and *Hubbell* to find that grand jury witness may assert his rights under the Fifth Amendment to questions seeking the password key to open his encrypted seized computer].)

For example, a defendant could participate in an online forum with thousands of members, a small minority of whom discuss anti-Government, violent, or otherwise criminal sentiments or activities. Providing his Internet browsing history would show that he had visited the forum, at which time a probation condition may require him to submit to a search of his participation on the social networking site, by providing his user name and password to that account. Because of the criminal activities or rhetoric espoused by some of the participants, appellant's association with the forum could itself be incriminatory.

Any incriminating testimonial acts provided by a defendant in adherence to his probation conditions would clearly be obtained by compulsion.

In *Minnesota v. Murphy* (1984) 465 U.S. 420, the United States Supreme Court upheld a probation condition requiring the probationer to "be truthful in all matters" because the probationer was still permitted to remain silent and therefore assert his Fifth Amendment right. (*Id.* at p. 427.) The Court observed that it was established that "'a State may not impose substantial penalties because a witness elects to exercise his Fifth Amendment right not to give incriminating testimony against himself.'" (*Id.*, at p. 434, citing *Lefkowitz v. Cunningham* (1977) 41 U.S. 801, 805.) The Court concluded that, "if the State, *either expressly or by implication*, asserts that invocation of the privilege would lead to revocation of probation, it would have created the classic penalty situation, the failure to assert the privilege would be excused, and the probationer's answers would be deemed compelled and inadmissible in a criminal prosecution." (*Id.* at p. 435, emphasis added.)

As noted above, probation conditions requiring a defendant to divulge his social activities online would effectually compel appellant to provide personally incriminating and testimonial acts. Yet failure to adhere to these conditions would lead to revocation of defendant's probation. Thus, defendant's communicative acts would be compelled because he is now in the "classic penalty" position of being required to choose between making statements which may be potentially incriminating, or jeopardizing his conditional liberty if he refuses to do so. (*Murphy, supra*, 465 U.S. at pp. 434-35; see

also *United States v. Bahr* (9th Cir. 2013) 730 F.3d 963, 966 ["Revocation of supervised release is not necessary to violate the right; *the threat of revocation is itself sufficient to violate the privilege* and make the resultant statements inadmissible."], italics added.)

For these reasons, if a defendant properly invoked his Fifth Amendment rights at sentencing, and the probation conditions are not coextensive with the protections of the Fifth Amendment, you should consider arguing that those probation conditions should be stricken.

Any argument raised against your client, positing that probationers may be compelled to waive their Fifth Amendment privilege against self-incrimination, can be contested as follows.

Fifth Amendment rights are not diminished when a person's liberty is constrained; if anything, those rights are enhanced. The California Supreme Court has provided that "the Fifth Amendment privilege attaches as soon as the defendant is in custody or even earlier, and does not depend on the commencement of custodial interrogation." (*People v. Tom* (2014) 59 Cal.4th 1210, 1224, citing *U.S. v. Velarde-Gomez* (9th Cir. 2001) 269 F.3d 1023, 1029 ["the government may not burden that right by commenting on the defendant's post-arrest silence at trial"]; *U.S. v. Moore* (1997) 104 F.3d 377, 385 ["neither *Miranda* nor any other case suggests that a defendant's protected right to remain silent attaches only upon the commencement of questioning as opposed to custody"]; *U.S. v. Burson* (10th Cir. 1991) 952 F.2d 1196, 1200 ["silence ... exhibited in a non-custodial interrogation" is protected by the 5th Amend.]; *State v. Mainaaupo* (2008) 178 P.3d 1, 18 [quoting *Velarde-Gomez* and *Moore*].)

Thus, a probationer's privilege to refuse to make statements that may tend to incriminate him remain intact, especially when he is in custody.

IV. Explanations and Illustrations of Relevant Terms[4]

a. Data Encryption

In cryptology (the study of secret writing), the original message that can be read by humans is called "plaintext," while the encrypted or unreadable message is called "ciphertext." The system of the transformation to ciphertext is called a "cryptologic system" or "cryptosystem." In modern encryption, a mathematical cryptosystem takes plaintext and encrypts it into ciphertext. Thus, when an encrypted message or data is sent or stored, what is being sent or stored is the ciphertext, not the plaintext. (Kiok, *Missing the Metaphor: Compulsory Decryption and the Fifth Amendment* (2015) 24 B.U. Pub. Int. L.J. 53, 55-56.)

One type of data encryption to which many of us might be familiar is known as SSL or Secure Sockets Layer. SSL is familiar, if not by name by the little "lock" icon

[4] PC Magazine has compiled a fantastic glossary of common technical and computer related terms, which can be found at: <http://www.pcmag.com/encyclopedia/index/a> [as of March 27, 2016].

that sometimes appears in a web browser. When the little lock appears, web pages are wrapped in a tunnel of encryption as they are downloaded. To use SSL, all a web surfer needs to do is visit a website hosted by a provider who provides SSL. (Ohm, *Law in a Networked World: Good Enough Privacy* (2008) 2008 U. Chi. Legal F. 1, 43, fn. 167.)

Many smartphones use data encryption technology. For example, BlackBerry is built with encryption as part of the base design. Enabling Content Protection on the BlackBerry will encrypt the device. If you use a BlackBerry Enterprise Server (BES), you enforce encryption as part of the security policy. (Nelson & Simek, *Technology; Hot Buttons: Security Tips for Smartphones* (2013) 39 Am. Bar. Ass'n 2, 22.) In late 2014, Apple and Google announced that iPhones and Android phones would be encrypted by default. (Weinstein, Drake, and Silverman, *Privacy vs. Public Safety: Prosecuting and Defending Criminal Cases in the Post-Snowden Era* (2015) 52 Am. Crim. L. Rev. 729, 738.)

Additionally, most personal computers and Operating Systems (Oss) have built-in encryption capabilities and can provide similar features: full-disk encryption as well as encrypting individual files or folders on a computer. All similarly provide "on-the-fly" encryption, which means that the software encrypts the hard drive such that the user enters the password a single time, and whenever a file or portion of the hard drive is accessed, the encryption software automatically decrypts the file or portion that is being accessed. When the computer is shut down, any plaintext files that were being viewed by the user are destroyed and only the ciphertext, or encrypted data remains. Thus, the language used when talking about "files," "folders," and "containers" being encrypted is misleading—unlike a real folder or container, the contents of an encrypted folder exist only in ciphertext, and not plaintext. Thus, if one is presented with an encrypted hard drive, the readable plaintext does not exist on the hard drive; only ciphertext exists. (*Missing the Metaphor*, *supra*, at pp. 56-60.)

b. End-to-End Encryption

You might hear the phrase "end-to-end" encryption in discussions regarding data encryption generally.

End-to-end encryption is a system of communication where the only people who can read the messages are the people communicating. No eavesdropper can access the cryptographic keys needed to decrypt the conversation—not even a company that runs the messaging service. (Greenberg, *Hacker Lexicon: What is End-to-End Encryption?* (Nov. 25, 2014) Wired Magazine < http://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/> [as of March 24, 2016].)

c. Metadata

Every electronic communication contains so-called content and non-content data. The audio of a phone call, the body of an email, and the characters in a text message fall in the "content" camp, for example. But for each communication, there is also a range of

non-content data associated with it, often referred to as "metadata." Phone calls generate logs with the phone company that track the numbers dialed, the length of the call, and the location of the caller. Every email contains a "header" full of metadata about how, when, and where the message is transmitted. It indicates who sent the message, who received it, and what it was about (depending on the descriptiveness of the subject line). (*Rethinking Privacy, supra*, 8 J. Nat'l Security L. & Pol'y at p. 274.)

d. Mobile Application Software or "Apps"

"Mobile application software on a cell phone, or 'apps,' offer a range of tools for managing detailed information about all aspects of a person's life. There are apps for Democratic Party news and Republican Party news; apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; apps for tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; apps for improving your romantic life." (*Riley, supra*, 134 S.Ct at p. 2490.)

e. Social Media

The phrase "social media" describes the online forms of communication that individuals and companies use to share information with interested parties (friends, colleagues, customers, etc.). Social media include microblogging sites such as Twitter and social networking sites such as Facebook. A primary feature of social media is that people actively follow someone who is posting content, and they are able to respond. For example, users can resend messages on Twitter and comment on posts in Facebook.

Ordinary blogs may allow feedback, and some Web sites do as well, but social media is all about spreading information to participating users. (PC Magazine, *Definition of: Social Media* < http://www.pcmag.com/encyclopedia/term/61162/social-media> [as of March 24, 2016].)

f. Social Networking Site

A "social networking site" is a Web site that provides a venue for people to share their activities with family, friends, and colleagues or to share their interest in a particular topic. Facebook, Google+, LinkedIn, and Twitter are the leading social sites.

Members create an online profile with biographical data, photos, and any other information they choose to post. They can communicate with each other in a blog-like format or via e-mail, instant messaging, or video chat. (PC Magazine, *Definition of: Social Networking Site* < http://www.pcmag.com/encyclopedia/term/55316/social-networking-site> [as of March 24, 2016].)

Although a user's personal profile is potentially viewable by anyone, the Web sites have privacy features that allow users to set limits on who may access their information and what information may be shared generally. Some web sites default their settings to allow broad public access, while others default to more private access. (*Malik*

J., *supra*, 240 Cal.App.4th at p. 903, citing Abilmouna, *Social Networking Sites: What an Entangled Web We Weave* (2012) 39 W. St. U. L. Rev. 99, 102.)

Conclusion

New opinions addressing issues of digital privacy are being issued practically every week. At the SDAP seminar, I will attempt to address new cases that emerge between the printing of this article and the subsequent presentation of this material, in person. If you have any questions, or just want to talk over these issues, please feel free to contact me at: nerissa@sdap.org.