2014 PA Super 145

COMMONWEALTH OF PENNSYLVANIA Appellant v. ADAM EDWARD STEM Appellee	IN THE SUPERIOR COURT OF PENNSYLVANIA No. 1275 WDA 2013

Appeal from the Order Entered on July 13, 2013
In the Court of Common Pleas of Westmoreland County
Criminal Division at No.: CP-65-CR-0004413-2012

BEFORE: FORD ELLIOTT, P.J.E., BOWES, J., and WECHT, J.

OPINION BY WECHT, J.: **FILED JULY 11, 2014**

The Commonwealth appeals the trial court's July 13, 2013 order granting appellee Adam Stem's motion to suppress pictures that were obtained from a warrantless search of Stem's cellular telephone, a search that was conducted incident to Stem's arrest for reasons unrelated to his cellular telephone. Because the United States Supreme Court recently held in ***Riley v. California***, ___ U.S. ___, 2014 WL 2864483 (2014), that such warrantless searches violate the Fourth Amendment to the United States Constitution, we affirm.

On August 14, 2012, Stem was arrested and charged with seventeen counts of possession of child pornography. 18 Pa.C.S. § 6312(d). Prior to trial, Stem filed a motion to suppress the pictures that were found on Stem's cellular telephone, and which formed the basis for the seventeen criminal counts against him. On April 30, 2013, the trial court held a hearing on

Stem's motion. The court summarized the evidence presented at that hearing as follows:

> [Allegheny Township police officer] Daniel Uncapher was the sole witness to testify. He stated that he has been employed as a police officer for Allegheny Township since 1993. On August 14, [2012,] he was working the afternoon shift in full uniform in a marked patrol vehicle. Officer Uncapher was familiar with Mr. Stem prior to August 14 of 2012.
>
> [Officer Uncapher] was dispatched to Sandalwood Apartments for a reported domestic [violence incident] involving [Stem] and Ashley Dale. Officer Uncapher had some recollection that [Stem's] name came up with a no trespass order at Sandalwood. Upon arrival at the apartment[,] Ashley Dale was uncooperative and would not respond to police about the whereabouts of [Stem]. Mr. Stem, however, answered [the officer's call] and the officer located him seated behind the kitchen sink. Officer Uncapher placed him into custody due to the fact that he believed there was a "no trespass order against him" [and] detained him for "criminal trespass inside the structure." When he placed [Stem] into custody, Officer Uncapher searched him and found a cell phone in his right front pocket. After [Stem] was handcuffed, he was placed in the back of the police cruiser. At that time, [Stem] was not free to leave, nor was he free to leave the police station while sitting in the processing room. It was clear that [Stem] was under arrest prior to Officer Uncapher looking at his cell phone. Officer Uncapher did not ask Mr. Stem for permission to search his cell phone after he was placed under arrest. At the police station, Officer Uncapher inspected [Stem's] cell phone. [Stem] was under arrest prior to Officer Uncapher turning on the phone and searching the cell phone data. The cell phone photos are not immediately displayed when the cell phone is turned on. To the contrary, the picture data must be accessed by proactively opening it. In order to do so, the picture icon must be touched. In the instant case, Officer Uncapher accessed the picture data by hitting the picture icon.

Trial Court Opinion ("T.C.O."), 7/16/2013, at 1-2 (citations to notes of testimony omitted). When Officer Uncapher accessed the picture data on

Stem's cellular telephone, the officer uncovered what appeared to be a photograph depicting child pornography. Based upon this discovery, Officer Uncapher applied for, and received, a search warrant that, when executed, revealed a total of seventeen photographs depicting child pornography.

On July 13, 2013, the trial court issued an opinion and a corresponding order granting Stem's motion to suppress the photographs located on the cellular telephone. On August 2, 2013, the Commonwealth filed a notice of appeal, wherein the Commonwealth certified that the trial court's July 13, 2013 order "will terminate or substantially handicap its ability to prosecute" Stem in accordance with Pa.R.A.P. 311(d). On August 30, 2013, the trial court directed the Commonwealth to file a concise statement of errors complained of on appeal pursuant to Pa.R.A.P. 1925(b). On August 26, 2013, the Commonwealth timely complied with the trial court's Rule 1925(b) order. On September 3, 2013, the trial court issued a statement pursuant to Pa.R.A.P. 1925(a) indicating that the Commonwealth's appeal lacks merit, and that the reasons supporting the court's conclusion appear in its July 13, 2013 opinion and order granting Stem's suppression motion.

The Commonwealth raises a single issue for our review: "Did the trial court err in suppressing images depicting child pornography discovered in [Stem's] lawfully seized cellular telephone?" Brief for the Commonwealth at 4.

Our standard of review in challenges to suppression orders is well-settled:

> Our standard of review in addressing a challenge to the denial of a suppression motion is limited to determining whether the suppression court's factual findings are supported by the record and whether the legal conclusions drawn from those facts are correct. Because the [defense] prevailed before the suppression court, we may consider only the evidence of the [defense] and so much of the evidence for the [Commonwealth] as remains uncontradicted when read in the context of the record as a whole. Where the suppression court's factual findings are supported by the record, we are bound by these findings and may reverse only if the court's legal conclusions are erroneous. . . . [T]he suppression court's legal conclusions are not binding on an appellate court, whose duty it is to determine if the suppression court properly applied the law to the facts. Thus, the conclusions of law of the courts below are subject to our plenary review.

Commonwealth v. Jones, 988 A.2d 649, 654 (Pa. 2010) (internal citations and quotation marks omitted).

The specific issue that we address in this case is whether a police officer may search the data contained on a modern day cellular telephone, often referred to as a "smart phone" due to the computer-like capabilities of the devices, without a warrant pursuant to the search incident to arrest exception to the warrant requirement prescribed in both the Fourth Amendment to the United States Constitution and Article I, Section 8 of the Pennsylvania Constitution. Very recently, the United States Supreme Court resolved this exact issue in a unanimous opinion in ***Riley***, and in ***Riley***'s companion case, ***Wurie v. United States***. The Court considered both cases in a consolidated opinion.

In ***Riley***, following a traffic stop, police determined that Riley did not have a valid driver's license. His car was impounded, and searched pursuant

to a valid inventory search. During the inventory search, police officers uncovered two firearms under the hood of the car. Riley then was arrested. Incident to arrest, the police seized Riley's cellular telephone from Riley's pants pocket.

> According to Riley's uncontradicted assertion, the phone was a "smart phone," a cell phone with a broad range of other functions based on advance computing capability, large storage capacity, and Internet connectivity. The officer accessed information on the phone and noticed that some words (presumably in text messages or a contact list) were preceded by the letters "CK"—a label that, he believed, stood for "Crip Killers," a slang term for members of the Bloods gang.
>
> At the police station about two hours after the arrest, a detective specializing in gangs further examined the contents of the phone. The detective testified that he "went through" Riley's phone "looking for evidence, because . . . gang members will often video themselves with guns or take pictures of themselves with guns." Although there was "a lot of stuff" on the phone, particular files that "caught [the detective's] eye" included videos of young men sparring while someone yelled encouragement using the moniker "Blood." The police also found photographs of Riley standing in front of a car they suspected had been involved in a shooting a few weeks earlier.

Riley, 2014 WL 2864483 at *4-5. California's attorney sought to use the gang-related information as an aggravated factor for the purposes of obtaining an enhanced sentence for Riley. Riley challenged the search in a motion to suppress, however, the California courts ultimately upheld the police actions. ***Id.*** at *5.

In ***Wurie***, the police observed Wurie engaging in what they believed to be a routine drug sale from a vehicle. Wurie was arrested and taken to the police station for booking. While there, the police retrieved two cellular

telephones from Wurie's person, one of which was a "'flip phone,' a kind of phone that is flipped open for use and that generally has a smaller range of features than a smart phone." ***Id.*** at *5. While in police custody, Wurie received repeated calls from "my house," which was displayed on the phone's external display screen. The police opened the phone and observed a photograph of a woman and a baby on the phone's "wallpaper." ***Id.*** The police then pressed a button to access the phone's call log, and, from there, was able to push other buttons to determine the phone number associated with the moniker "my house." The police then used an online phone directory to trace the number to an apartment building, for which police later obtained and executed a search warrant. During the search of Wurie's apartment, the police recovered crack cocaine, marijuana, drug paraphernalia, a firearm with ammunition, and United States currency. ***Id.*** In a suppression motion, Wurie challenged the constitutionality of the search of his flip phone. The District Court denied the motion. However, the First Circuit Court of Appeals reversed the District Court, and ordered the fruits of the search to be suppressed. ***Id.*** at *6.

The Supreme Court granted certiorari on both cases, consolidated them for a single opinion, and reversed the California courts in ***Riley***, and affirmed the First Circuit in ***Wurie***. ***Id.*** at *20. The Court began its analysis with a discussion of the well-settled history and parameters of the search incident to an arrest exception to the warrant requirement. The Court explained that the exception permits an arresting officer without a warrant

to search an arrestee's person and the area within his immediate control only for personal property immediately associated with the arrestee. ***Id.*** at ___ (citing, *inter alia*, ***Chimel v. California***, 395 U.S. 752 (1969); ***United States v. Robinson***, 414 U.S. 218 (1973); and ***Arizona v. Gant***, 556 U.S. 332, 343 (2009) (limiting search incident to arrest exception in the vehicle context to when "the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search."). The Court reiterated the well-established dual bases that justify the exception: ensuring police safety and preventing the destruction of evidence. ***Id.*** at *6-8.

The Court proceeded to consider "how the search incident to arrest doctrine applies to modern cell phones, which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." ***Id.*** at *9. The Court held that the doctrine cannot be extended to such devices, and held "instead that officers must generally secure a warrant before conducting such a search." ***Id.***

In so holding, the Court first considered the interplay between the two principal concerns underlying the search incident to arrest exception, police safety and preservation of evidence, and modern cellular devices, beginning with police safety. The Court first rejected the notion that such a device, by its very nature, poses a threat to a police officer, stating that:

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

Id. at *10. The Court also spurned the argument that cellular devices may be used to ensure police safety by more indirect means, such as by alerting officers that another individual with a criminal mindset may be heading to the scene with the intent to harm the officers. The Court recognized that the government has a strong interest in thwarting such possibilities, but noted that no evidence existed to suggest that such concerns were based upon real life experiences. Moreover, the Court noted that the exception is narrow, and generally limited to dangers posed by the arrestee himself, and that outside threats do not "lurk in all custodial arrests." ***Id.*** (citing ***United States v. Chadwick***, 433 U.S. 1, 14-15 (1977)). "Accordingly, the interest in protecting officer safety does not justify dispensing with the warrant requirement across the board." ***Id.***[1]

---

[1] In reaching this conclusion, the Court noted that, when such outside threats become a real possibility, accessing the cellular device without a warrant may be addressed more appropriately under one of the "case-specific exceptions to the warrant requirement, such as the one for exigent circumstances." ***Id.*** at *10 (citing ***Warden, Md. Penitentiary v. Hayden***, 387 U.S. 294, 298-99 (1967)).

The Court then turned its attention to the second rationale, and the one that the United States and California primarily focused upon, the prevention of the destruction of evidence. The Court noted that both Riley and Wurie conceded that the police constitutionally were permitted to seize and secure their telephones in order to prevent the destruction of evidence **during the time it takes to obtain a valid search warrant**. ***Id.*** Observing that this concession was "sensible," the Court immediately concluded that "once law enforcement officers have secured a cell phone, there is no longer any risk that the arrestee himself will be able to delete incriminating data from the phone." ***Id.***

Nonetheless, the United States and California both argued that cellular devices were susceptible to two types of destruction of data that are unique to these devices: remote wiping and data encryption. Remote wiping "occurs when a phone, connected to a wireless network, receives a signal that erases stored data," which can happen when a third party sends a remote signal to the phone. ***Id.*** at *11. Encryption is a security feature on cellular telephones that, when the phones are locked, the "data becomes protected by sophisticated encryption that renders a phone all but 'unbreakable' unless police know the password." ***Id.*** The Court rejected both concerns, noting, *inter alia*, that the Court had been "given little reason to believe that either problem is prevalent." ***Id.*** Moreover, with respect to remote wiping, the Court determined that the problem easily, and fully, can be prevented simply by disconnecting the phone from the network on which

the phone is operating. Or, the Court explained, cellular telephones can be protected from either remote wiping or encryption by placing the devices into "Faraday bags," which essentially are "sandwich bags made of aluminum foil that isolate the devices from radio waves." ***Id.*** at *12.[2]

Having determined that searching cellular telephones after an arrest does not satisfy the traditional dual bases underlying the search incident to arrest exception, the Court turned its attention to the governments' argument that searching a cellphone is materially indistinguishable from seizing and searching items incident to arrest that contain the same information as the data stored on a cellular telephone, but in physical form. For instance, a police officer may search a woman's purse incident to arrest and, for example, review the contents of a date book that includes phone numbers and addresses. The United States argued that, in this type of scenario, the phone number directory in a cellular device should not be considered different from the date book in the woman's purse, and, therefore, should be susceptible to a search incident to arrest. In response, the Court stated that this argument is "like saying riding on horseback is materially indistinguishable from a flight to the moon. Both are ways of

---

[2] The Court again reminded law enforcement that, if police are truly concerned with a "now or never" situation with regard to remote wiping or encryption, the exigent circumstances exception may be available to justify searching a cellular telephone immediately after an arrest. ***Id.*** at *12.

getting from point A to point B, but little else justifies lumping them together." ***Id.*** at *13.

The Court, in large part, focused upon the interplay between modern day cellular devices and the privacy interests of the arrestee. The Court's discussion on this essential point, in relevant part, follows:

> Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse. A conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom.
>
> Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.
>
> One of the most notable distinguishing features of modern cell phones is their immense storage capacity. . . . The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs, labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.

> Finally, there is an element of pervasiveness that characterizes cell phones but not physical records. Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception. . . . [I]t is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate. Allowing police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case.
>
> Although the data stored on a cell phone is distinguished from physical records, by quantity alone, certain types of data are also qualitatively different. An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD. Data on a cell phone can also reveal where a person has been.
>
> * * *
>
> In 1926, Learned Hand observed . . . that it is "a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him." ***United States v. Kirschenblatt***, 16 F.2d 202, 203 [(2d Cir. 1926)]. If his pockets contain a cell phone, however, that is no longer true. Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.
>
> To further complicate the scope of the privacy interests at stake, the data a user views on many modern cell phones may not in fact be stored on the device itself. . . . Cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself. Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference. . . . [T]he Government proposes that law enforcement agencies "develop protocols to address" concerns

> raised by cloud computing. Probably a good idea, but the Founders did not fight a revolution to gain the right to government agency protocols.

Id. at *13-16 (most citations and all footnotes omitted).

Finally, the Court recognized that its decision "will have an impact on the ability of law enforcement to combat crime," but nonetheless reminded us that "[p]rivacy comes at a cost." ***Id.*** at *19. The Court concluded as follows:

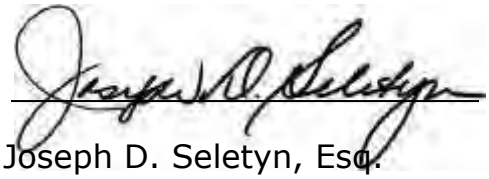
> Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life." The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.

Id. at *19 (citation omitted).

In light of the Court's decision in ***Riley***, the search of Stem's cellular telephone undoubtedly was unconstitutional. The Commonwealth herein echoes many of the same arguments that the Supreme Court heard, and rejected, in ***Riley***. Our recitation above of the essential discussions from ***Riley*** serves well to dispose of those arguments, and we need not rehash those here. Accordingly, we affirm the trial court's order suppressing the evidence obtained from Stem's cellular telephone, and the fruits derived therefrom.

Order affirmed.

Judgment Entered.



Joseph D. Seletyn, Esq.
Prothonotary

Date: 7/11/2014