

2021 PA Super 204

COMMONWEALTH OF PENNSYLVANIA	:	IN THE SUPERIOR COURT OF
	:	PENNSYLVANIA
Appellant	:	
	:	
v.	:	
	:	
TOD A. GALLAGHER	:	No. 1529 WDA 2019

Appeal from the Order Entered September 23, 2019
 In the Court of Common Pleas of Butler County Criminal Division at
 No(s): CP-10-CR-0000407-2019

BEFORE: PANELLA, P.J., BENDER, P.J.E., BOWES, J., LAZARUS, J., OLSON, J., DUBOW, J., KUNSELMAN, J., MURRAY, J., and McCAFFERY, J.

OPINION BY McCaffery, J.: **FILED: OCTOBER 12, 2021**

The Commonwealth appeals from the Butler County Court of Common Pleas' order of suppression. This matter, which is before the Court *en banc* after this Court granted reargument, raises an important question as to what police must do to obtain a knowing and voluntary consent to search by permission all or part of a cellular phone's data. The Commonwealth argues that it established that Appellee Tod A. Gallagher (Gallagher) gave such consent and the trial court erred in finding otherwise. Because the Commonwealth has not established meaningful consent to the invasive search it performed, we affirm.

The trial court summarized the underlying facts as follows:

At [the motions] hearing, Patrolman Chris Kopas ["Patrolman Kopas"] testified that he has been employed with the Adams Township Police Department for five[-]and[-]a[-]half years []. He testified that on November 9, 2014[,], at 1:42 a.m., he responded to a 911 dispatch from a female caller reporting an

attempted kidnapping who [sic] had escaped and was hiding. The female caller was 16[]years[]old and reported that she had a head injury. Patrolman Kopas proceeded to the location[,] which was in the general location of the self-storage units on Mars-Evans City Road in the township. The patrolman found the female and reported that she was hysterical, panicky[,] and scared. An EMS unit responded to check her well-being and[,] during that time, [the victim] told the patrolman that she was picked up in McKeesport by [Gallagher] and Cody Seagriff [(“Seagriff”)] earlier in the evening. They stopped at a gas station and the Evans City Cemetery[,] where they drank alcohol, after which they went to 1260 Mars-Evans City Road to see Joe Perkins [(“Perkins”)]. The female next reported that she woke up on the side of a road with someone on top of her and their hand down the front of her pants. She claimed that her pants and underwear were pulled down. She was able to get away and hid in the woods.

. . .

The victim believed the individual who was on top of her was [Gallagher]. The victim was transported to UPMC Cranberry to conduct a sexual assault examination.

Trial Ct. Op., 9/30/19, at 1-2.

Gallagher was arrested under suspicion for driving under the influence. He was informed of his rights under **Miranda**,¹ and interviewed for about one-half hour until his father arrived to take him home. The trial court offers the following summary of what happened next:

At [the] hearing, Detective Michael Bailey [(“Detective Bailey”)] [] testified. He has been employed as a police officer for approximately seventeen (17) years and was assigned to investigate this case. Patrolman Kopas informed the detective of the allegations and evidence collected. [Detective] Bailey contacted [Gallagher] on November 18, 2014[,] and left a message. [Gallagher] came to the station on November 19, 2014[,] to talk about the incident. Det[ective] Bailey informed

¹ **See *Miranda v. Arizona***, 384 U.S. 436 (1966).

[Gallagher] that he was not under arrest and that he was free to leave at any time. [Gallagher] agreed to have a conversation.

Det[ective] Bailey asked [Gallagher] if he could look at his cell phone. [Gallagher] did not object and showed [Detective Bailey] a picture of the two girls that he was with the previous weekend. Commonwealth's Exhibit "2" is the township's consent form to search stored electronic media. [Gallagher] signed it on November 19, 2014

Id. at 2-3.

The consent form stated, in full:

CONSENT TO SEARCH OF STORED ELECTRONIC MEDIA

I [Tod Gallagher, handwritten] **having been advised of my rights by [Michael Bailey, handwritten], consent to having my computer hardware and all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data [sic].** Hardware includes (but is not limited to) any data-processing devices (such as central processing units, memory typewriters, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices (such as fixed disks, external hard disk drives and diskettes, tape drives and tapes, optical storage devices, transistor-like binary devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, plotters, video display monitors, and optical readers); cell phones, pagers, PDA"s [sic] (personal desktop assistants) and related communications devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware such as physical keys and locks).

Consent to Search of Stored Electronic Media (single page), 11/19/14
(emphasis added).

Gallagher, who was charged with attempted rape and related charges,² filed an omnibus pretrial motion on June 19, 2019, seeking (*inter alia*) suppression of evidence gleaned from the “phone dump” conducted by police during the interview described above. The trial court conducted a hearing on July 22, 2019. The court granted, in part, Gallagher’s pretrial suppression motion, suppressing all evidence seized from Gallagher’s cell phone. The Commonwealth filed the instant timely appeal, certifying per Pa.R.A.P. 311(d) that the suppression order substantially handicapped its prosecution, and timely complied with the trial court’s order per Pa.R.A.P. 1925(b). On October 28, 2020, a three-member panel of this Court affirmed the order of suppression, with one Judge concurring in part and dissenting in part. On December 29, 2020, this Court granted the Commonwealth’s Application for Reargument, which was filed on November 6, 2020.

On reargument, the Commonwealth presents the following claim for our review:

[W]hether the record supports the trial court’s finding that . . . Appellee did not knowingly consent to the search and seizure of the stored cell phone data.

Commonwealth’s Rearg. Brief at 1.

We apply the standard and scope of review as articulated by our Supreme Court:

² 18 Pa.C.S. § 901(a), where the attempted crime is 18 Pa.C.S. § 3121(a)(1).

When reviewing a ruling on a motion to suppress, this Court is bound by the factual findings made by the suppression court that are supported by the record but review its legal conclusions *de novo*. [] Our scope of review is limited to the record developed at the suppression hearing, considering the evidence presented by the . . . the prevailing party and any uncontradicted evidence presented by [the party bringing the appeal].

Commonwealth v. Fulton, 179 A.3d 475, 487 (Pa. 2018) (citations omitted).

The Commonwealth argues that under the circumstances surrounding Gallagher's alleged consent to search his phone, "it is rather obvious that the right to refuse the search was known" to Gallagher. Commonwealth's Rearg. Brief at 2-3. "Common sense and a view of the surrounding situation would indicate to any reasonable, semi[-]intelligent person that if a request is being made of him, the converse option is also a possible right available to him." **Id.** at 3.

Gallagher points out that the consent form given to him "did not advise [him] what his rights were, and Detective Bailey never told [him] that he was free to leave and free to [withhold] consent." Gallagher's Rearg. Brief at 5. "Detective Bailey's testimony is consistent with him basically asking [Gallagher] if he could look at his phone [but the] record is far from clear as to whether [Gallagher] ever consented, voluntarily or involuntarily, to a search of all data on his phone." **Id.**

The trial court noted, in support of its conclusion that "the Commonwealth did not establish that [Gallagher] consented to the cell phone dump," that the form used by detectives "fails to explain [Gallagher's] rights

with regard to the stored data,” and “the form fails to explain what [Gallagher was] consenting to.” Trial Ct. Op., 9/30/19, at 3. In its opinion per Pa.R.A.P. 1925(a), the trial court cited **Schneckloth v. Bustamonte**, 412 U.S. 218, 249 (1973), for the principle that voluntariness is a question of fact to be determined from the relevant circumstances of the search and consent thereto. Trial Ct. Op., 11/19/19, at 1. “We hold [] that when the subject of a search is not in custody and the State attempts to justify a search on the basis of his consent, the Fourth and Fourteenth Amendments require that it demonstrate that the consent was in fact voluntarily given, and not the result of duress or coercion, express or implied.” **Schneckloth**, 412 U.S. at 248.

In **Fulton**, our Supreme Court applied Supreme Court of the United States precedent in reaching the conclusion that “accessing any information from a cell phone without a warrant contravenes the United States Supreme Court’s decision in **Riley v. California** and **United States v. Wurie**, 573 U.S. 373 (2014) (hereinafter, “**Riley/Wurie**”).” **Fulton**, 179 A.3d at 479.³

The **Riley/Wurie** Court described cell phones as “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” and as “based

³ In **Riley/Wurie**, the Supreme Court held that police generally must obtain a warrant to search digital information from a cell phone seized incident to arrest. **Riley/Wurie**, 573 U.S. at 403 (“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.”).

on technology nearly inconceivable just a few decades ago”

Riley/Wurie, 573 U.S. at 385.

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 current top-selling smart phone has a standard capacity of 16 gigabytes (and is available with up to 64 gigabytes). Sixteen gigabytes translates to millions of pages of text, thousands of pictures, or hundreds of videos. [] Cell phones couple that capacity with the ability to store many different types of information: Even the most basic phones that sell for less than \$20 might hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on. . . . We expect that the gulf between physical practicability and digital capacity will only continue to widen in the future.

The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone’s capacity allows even just one type of information to convey far more than previously possible. **The sum of an individual’s private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions**; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.

Finally, there is an element of pervasiveness that characterizes cell phones but not physical records. Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception. According to one poll, nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower. [] A decade ago police officers searching an arrestee might have occasionally stumbled across a highly personal item such as a diary. [] But those discoveries were likely to be few and far between. Today, by contrast, it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate. [] Allowing the police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case.

Id. at 393-95 (emphasis added; citations and footnotes omitted). The Court pointed out that cell phones also allow users (and police) to access yet more data kept in “cloud computing” storage, thus offering up potentially unlimited quantities and types of data touching upon every area of the user’s life. **Id.** at 397.

That Court also observed that officers who are concerned that a sophisticated subject of investigation might be able to render data stored on a cell phone inaccessible (by data wiping or encryption) “can turn the phone off or remove its battery” or can place the phone in a Faraday bag where the

phone is completely isolated from any external signal that would alter or omit data.⁴ **Riley/Wurie**, 573 U.S. at 390.

“The burden of proving a valid consent to search, since it represents a waiver of a substantial constitutional right, rests with the Commonwealth; and, the courts will indulge every reasonable presumption against such waiver.” **Commonwealth v. Griffin**, 336 A.2d 419, 421 (Pa. Super. 1975). “[V]oluntariness may be established by the Commonwealth if all the facts and circumstances indicate that the consent was voluntarily given.” **Id.**

The suppression notes reflect that the investigating officer, Detective Bailey, testified that Gallagher showed him a photograph that was stored on his phone, and the officer then asked Gallagher “if he minded if we looked at his phone.” N.T. Suppression, 7/22/19, at 31. Gallagher was then asked to sign a consent form regarding electronic media. **Id.** Based on the question Gallagher was asked in the context of their conversation, it is far from clear that “looking at” his phone would include a complete data dump, as opposed to flipping through his photograph folder, which is what Gallagher was doing when the officer asked if Gallagher would mind if he “looked at” it. If a person is showing another a certain feature or application on their phone and was asked “hey, can I look at that?”, it would be reasonable to assume that they were being asked about that particular feature or application (in this situation,

⁴ Faraday bags are “essentially sandwich bags made of aluminum foil: cheap, lightweight, and easy to use” in preventing external signals to reach the cell phone stored therein. **Riley/Wurie**, 573 U.S. at 390.

the photograph application) as opposed to a global capture of all data on the device. One who consents to a search retains the right to control the scope of consent given; this is intrinsic to the nature of consent and the consent exception to the warrant requirement. "A person's right to delimit the scope of consent to a search is well established." ***Commonwealth v. Guerrero***, 646 A.2d 585, 587 (Pa. Super. 1994) (citation omitted).

Because the verbal exchange did not put Gallagher on notice as to the true scope of the search sought, the trial court properly focused next on the form Gallagher was given and asked to sign. The trial court concluded as follows:

[Detective] Bailey explained that he did not advise [Gallagher] of his rights with respect to his cell phone and acknowledged that the form submitted . . . does not explain those rights either. [] The form appears to be incomplete in that the heading of the form states, "CONSENT TO SEARCH STORED ELECTRONIC MEDIA", but the actual wording of the document neither explains the rights which a person is waiving nor what they are in fact consenting to. The record reflects that [Gallagher] was never advised of his constitutional right to privacy of the data stored in his cell phone and that he was free to deny the request for consent to search.

Trial Ct. Op., 11/19/19, at 3. We can find no basis to disturb the trial court's factual findings as to the form in question.⁵ Without knowing the true scope

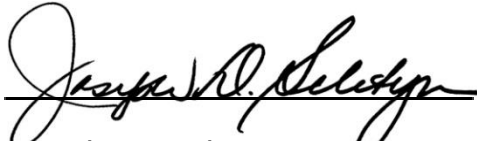
⁵ The form does not mention any rights the subject of an investigation has. It focuses, rather, on covering a broad variety of electronic items, including "memory typewriters" and pagers. Consent to Search of Stored Electronic Media. It does not put the subject on notice as to the type of data that police may glean. The critical sentence as to consent is itself incomplete: "I, [space for handwritten name], having been advised of my rights by [space for
(Footnote Continued Next Page)

of consent sought and the nature and extent of rights he was waiving, it is hard to see how Gallagher could have made a knowing, voluntary waiver of those rights and consent to a total capture of all cell phone data, including data he may not have known the phone contained.

Given the totality of the circumstances, neither the verbal exchange nor the form Gallagher was given can establish, as the Commonwealth must, that Gallagher made a knowing and voluntary waiver of his rights as to the cell phone. Therefore, we must affirm the order of suppression.

Order affirmed.

Judgment Entered.

A handwritten signature in black ink, appearing to read "Joseph D. Seletyn", written over a horizontal line.

Joseph D. Seletyn, Esq.
Prothonotary

Date: 10/12/2021

officer's name], consent to having my computer hardware and all equipment which can collect, analyze, create, display, convert store, conceal, or transmit electronic magnetic, optical, or similar computer impulses or data." **Id.** The sentence does not say what they consent to having done with their hardware, as the sentence is incomplete. Although the form indicates that the named officer advised the named subject of their rights, that did not occur here.