

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

In the Matter of the Search Warrant
Application for the Search of a Townhome
Unit

Case No. 20 MC 106

Magistrate Judge Sunil R Harjani

MEMORANDUM OPINION & ORDER

The government has presented an application for a warrant to search a townhome for evidence of trafficking in counterfeit United States currency. Among the items identified by the government for search and seizure are electronic devices located in the premises. More specifically, the government's application seeks to seize electronic devices in the premises that are connected to the subject offense or in the possession of the target of the offense. The Court has determined that this limitation on the scope of the seizure of electronic devices is consistent with the Supreme Court's Fourth Amendment jurisprudence, and in particular, *Riley v. California*, 573 U.S. 373 (2014), and thus has authorized the warrant. The Court issues this opinion to explain the reasons why it has authorized a warrant with this limitation.¹

Background

The government seized a package coming from overseas, which was addressed to a townhome in this district. A customs officer searched the mail parcel and found that it contained thousands of dollars in counterfeit United States currency. The government has consequently submitted an application requesting authorization to install an electronic tracker on or inside the

¹The search warrant was authorized and signed by the Court on February 7, 2020 and continues to remain under seal in this matter. The Court has ensured that information in this opinion, which is not under seal, does not reveal confidential details about the investigation.

mail parcel and seeks to monitor the transmission of the tracking device while the mail parcel is in public and private areas. In connection with the electronic tracker, the government has asked for an anticipatory search warrant to search the addressee townhome unit for evidence, instrumentalities, fruits, and contraband associated with the possession and importation of counterfeit currency, once the parcel is received at the townhome or opened at townhome. *See* 18 U.S.C. §§ 472 & 480. Attached to the government's application, in its list of items to be seized at the premises, the government has identified the mail parcel; various documents and records relating to counterfeit currency, such as photographs, notes, ledgers, items that can print counterfeit currency, contact information for individuals involved in the offense, and records on the possession or importation of counterfeit currency; as well as "[e]lectronically-stored data from devices reasonably believed to be possessed or used by [the suspect] or linked to the Subject Offenses," which will be searched only for the items listed above.

Discussion

The issue presented here concerns the scope of law enforcement's ability to seize electronic devices during a search executed pursuant to a warrant. The Northern District of Illinois has established a search protocol for the seizure of electronic devices. Consistent with Federal Rule of Criminal Procedure 41(e)(2)(B), the protocol allows the government to immediately remove from the premises electronic devices that are authorized for seizure pursuant to a search warrant, download the data and search for the specific items to be seized within 30 days, and then return all removed electronic devices to the premises. This written protocol, as permitted by Rule 41(e)(2)(B), is attached to all search warrants that authorize the seizure of electronic devices in this district. The protocol is a consequence of the practical difficulties in downloading all data in multiple electronic devices on site during the execution of the search warrant. The protocol also

accounts for the extra time needed to search the devices for the specific items for which there is probable cause to seize, such as ledgers of narcotics transactions or fraudulent financial statements, among multiple gigabytes of information of irrelevant information that may be stored on an electronic device. To be clear, the seizure of the electronic devices is temporary, but it allows the government time to search for and copy the specific items related to the offense, if any, among the entire set of data that is contained on that device.

Before *Riley*, the government would often seek authorization to remove every electronic device located in the premises, and then conduct a search for the specific items related to the offense. This broad language authorized the seizure of all cell phones in the premises, including those that were not connected to the targets of the investigation. For example, if a premises was occupied by a family of four, the warrant's broad authorization would include the seizure of the children's iPhones and iPads as well. In general, the traditional view of searching a premises was viewed as applicable to electronic devices, which is that agents may search the entirety of the premises as long as it was capable of containing the item to be seized. *United States v. Ross*, 456 U.S. 798, 821 (1982) (“[A] warrant that authorizes an officer to search a home for illegal weapons also provides authority to open closets, chests, drawers, and containers in which the weapon might be found.”). Indeed, pre-*Riley*, the rationale made sense—if the government could search the most private parts of a home, such as bedroom closets and drawers, for evidence of a crime, surely the government could also search all electronic devices located in the premises. Moreover, law enforcement would not necessarily know which electronic devices in the premises stored evidence of the offense, which necessitated reviewing all electronic devices. During the execution of a search warrant, law enforcement often find multiple cell phones, iPads, desktop and laptop computers, external hard drives and thumb drives, along with other smart devices in residences,

which are all capable of storing immense amounts of data. Thus, the search of all devices was viewed as akin to searching every room of the house, even the guest bedroom, rather than only the perpetrator's bedroom or home office, because evidence could easily be stored anywhere in the home. An important difference, however, was that once in the bedroom, the government could only seize and remove items connected to the offense that were specifically covered by the warrant. In the case of electronic devices, there remained and continues to remain, a greater intrusion of an individual's privacy interests in the procedure laid out by Rule 41(e)(2)(B) and this district's protocol, in that the individuals in the premises are temporarily deprived of the electronic device, and its entire contents, for approximately 30 days, and not simply the specific data that is tied to the offense. However, as stated above, the impracticality of on-site data duplication and searching made treating electronic devices in this manner necessary, and Rule 41(e)(2)(B) was amended in 2009 to account for this necessity. *See* Fed. R. Crim. P. 41(e)(2) advisory committee's note to 2009 amendment.

The Supreme Court's decision in *Riley*, and its recognition that cell phones in particular must be treated differently, has changed the calculus of authorizing seizures of every electronic device located in a premises. In *Riley*, the Supreme Court held that the government must seek a warrant to search cell phones that were seized incident to an arrest. In so doing, the Supreme Court described the unique nature of cell phones in the modern era, and distinguished those items from other objects that are traditionally the subject of a search incident to arrest. The Supreme Court stated: "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.” 573 U.S. at 393. The Supreme Court further noted the immense storage capacity of a cell phone, and acknowledged several consequences for privacy interests: “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.” *Id.* at 394. In addition, the Court recognized the capacity of cell phones to store internet browsing history, cell location information, and applications that store data in the cloud and not just on the physical device itself. *Id.* at 395-96. In elaborating on the breadth of private data available on a phone, the Supreme Court made this relevant observation: “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.” *Id.* at 396-97.

Thus, while *Riley* involved whether the government could engage in a warrantless search of a cell phone incident to arrest, its discussion about the extensive amount of personal data available on the phone, much more than would be located in one’s home, is instructive on how the Supreme Court views searches of cell phones in the modern era. Indeed, if cell phones contain more personal and private data than what is located in the home in non-digital form, it begs the question of whether the mere presence of a cell phone in a premises, without more, is sufficient to

bring that phone within the scope of a search and seizure. *Riley*'s discussion about the unique nature of a cell phone as a device that stores essentially all data of modern life necessitates questioning whether a cell phone can be removed from the premises without probable cause that connects that specific phone to the crime or the perpetrators of the offense.

Such a question was raised by the United States Court of Appeals for the D.C. Circuit in *United States v. Griffith*, 867 F.3d 1265 (D.C. Cir. 2017). There, the Court held that a search warrant authorizing the seizure of all cell phones and electronic devices found in the defendant's residence was unsupported by probable cause. Specifically, in *Griffith*, law enforcement obtained a warrant to search the defendant's residence in connection with their investigation of a homicide committed more than one year earlier. *Id.* at 1268. Investigators suspected that the defendant had driven the getaway car after the homicide. *Id.* at 1268-69. The warrant authorized the search and seizure of "all electronic devices" found in the defendant's residence, including all cell phones. *Id.* at 1269. The Court held that the warrant affidavit failed to demonstrate probable cause for any of the items sought to be seized, as it conveyed no reason to think that the defendant owned a cell phone, that the cell phone would likely be found in his residence, or that any phone would be likely to contain incriminating evidence. *Id.* at 1272-74. The Court also held that the warrant was overbroad in its authorization of the seizure of all electronic devices found in the residence, given the officers' justification for entering the home—to recover any devices *owned by the defendant*. *Id.* at 1276. In finding overbreadth, the Court determined that the warrant authorized law enforcement to seize not only the defendant's phone, but also his girlfriend's phone, as she lived in the premises with him. *Id.* In distinguishing cell phones, the Court recognized the latitude that agents have in seizing items that are contraband, such as narcotics, but recognized that cell phones were lawful and innocuous objects. *Id.* As a result, the court held that "the warrant should have

limited the scope of permissible seizure to devices owned by Griffith, or devices linked to the shooting.” *Id.*

Griffith presented a unique situation because the warrant in that case authorized the seizure of all electronic devices with no stated probable cause that cell phones were even used in the commission of a crime or would be located in the premises, and the crime had occurred more than a year prior to the issuance of the warrant. As a result, *Griffith* represents an unusual set of facts where there were multiple, significant constitutional problems with the search warrant. Nevertheless, *Griffith*’s limitation on the seizure of all electronic devices without specific probable cause that the devices were linked to the offense or possessed by the target of the offense is instructive. Since *Griffith*, courts, in distinguishing the facts in *Griffith*, have upheld warrants that authorize the seizure of electronic devices that are more directly tied to the offense or the alleged perpetrator of the offense. *See, e.g., United States v. Manafort*, 314 F. Supp. 3d 258, 265-66 (D.D.C. 2018) (distinguishing *Griffith* because warrant at hand approved the seizure of devices that had been used in specific offenses); *United States v. Manafort*, 323 F. Supp. 3d 795, 803–04 (E.D. Va. 2018) (distinguishing *Griffith* on basis that agents “had reason to believe that electronic devices belonging not just to defendant, but also to defendant’s wife, would contain evidence of the Subject Offenses”).

In this Court’s view, *Riley* and *Griffith* counsel caution before a court authorizes seizure of all electronic devices from a premises. The Fourth Amendment requires not only that warrants be supported by probable cause, but that they “particularly describ[e] the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. The particularity requirement “ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.” *Maryland v. Garrison*,

480 U.S. 79, 84 (1987); *see also Marron v. United States*, 275 U.S. 192, 196 (1927) (“The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another.”). An application for a search warrant concerning property or possessions must demonstrate cause to believe that “relevant evidence will be found in the place to be searched.” *Michigan v. Clifford*, 464 U.S. 287, 294 (1984). *See Safford Unified Sch. Dist. No. 1 v. Redding*, 557 U.S. 364, 370 (2009); *Illinois v. Gates*, 462 U.S. 213, 238 (1983). Moreover, “[t]here must, of course, be a nexus . . . between the item to be seized and criminal behavior.” *Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294, 307 (1967). A warrant with an “indiscriminate sweep” is “constitutionally intolerable.” *Stanford v. Texas*, 379 U.S. 476, 486 (1965).

Besides the need for particularity, the Supreme Court’s Fourth Amendment jurisprudence has consistently recognized the heightened privacy interests that individuals have in their homes. “[W]hen it comes to the Fourth Amendment, the home is first among equals.” *Florida v. Jardines*, 569 U.S. 1, 6 (2013). “At the Amendment’s ‘very core’ stands ‘the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.’” *Id.* (quoting *Silverman v. United States*, 365 U.S. 505, 511, 81 S.Ct. 679, 5 L.Ed.2d 734 (1961)). “The Founding generation crafted the Fourth Amendment as a 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.” *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018) (internal quotation marks and citations omitted). Furthermore, the Supreme Court has also recognized the need to proceed with caution when new technology could result in an unreasonable invasion of an individual’s privacy interests in his home. *See Kyllo v. United States*, 533 U.S. 27 (2001) (holding that thermal imaging of an individual’s home

constituted a search and therefore required a warrant).

Riley has now added cell phones to this highly protected category given the device's ability to store essentially the entirety of a person's life in digital form on one device. See *United States v. Wanjiku*, 919 F.3d 472, 484 (7th Cir. 2019) (recognizing that *Riley* and *Carpenter* support the argument that "the Supreme Court has recently granted heightened protection to cell phone data.") Indeed, so prevalent are these devices that the Supreme Court stated that a cell phone, to an outsider, would be viewed as "an important feature of human anatomy." *Riley*, 573 U.S. at 385. As a result, the search and seizure of a cell phone that is found within an individual's home is essentially a "one-two punch." In other words, it is hard to imagine a more intrusive invasion of an individual's privacy interests than searching the entire contents of a person's cell phone located within the confines of a home. See e.g. *United States v. Oglesby*, No. 4:18-CR-0626, 2019 WL 1877228, at *5 (S.D. Tex. Apr. 26, 2019) ("[T]his Court concludes that the protections given to a cell phone must be at least equal to, if not greater than, the protections set out for houses."); *Huff v. Harness*, No. 3:16-CV-164-DPM, 2018 WL 2434329, at *1 (E.D. Ark. May 30, 2018) (interpreting *Riley*, observing, "[o]ur cell phones are home-like because, by choice and by default, we live inside them").

The Court finds that the warrant at issue here is not overbroad because it limits the seizure of electronic devices to those that are linked to the offense or the perpetrator of the offense. First, there is probable cause to seize and search electronic devices because the government's affidavit included facts demonstrating that the suspect had likely used an electronic device to access a website in order to purchase the counterfeit currency. Second, the government has limited the electronic devices that it can search and seize, and thus the enhanced privacy considerations discussed in *Riley* are satisfied. Specifically, the warrant authorizes seizure of electronic devices

that are “reasonably believed to be possessed or used by [the suspect] or linked to the Subject Offenses[.]” As discussed above, this is a reasonable limitation on the scope of the warrant because the search and seizure is directly tied to the offense or its perpetrator. *See Riley*, 573 U.S. 381 (“As the text of [the Fourth Amendment] makes clear, the ultimate touchstone of the Fourth Amendment is reasonableness.”) (internal quotations omitted); *see Matter of Residence in Oakland, California*, 354 F. Supp. 3d 1010, 1014 (N.D. Cal. 2019) (search warrant for electronic devices must be limited to “devices reasonably believed by law enforcement to be owned or controlled by the two suspects identified in the affidavit”). Once seized, law enforcement can then search the contents of those electronic devices for data related to the offense and specifically identified in Attachment B of the warrant. These items identified in Attachment B include documents, receipts, notes, ledgers, photographs, and other records relating to counterfeit currency. Under this formulation, law enforcement cannot remove and search every electronic device found in the premises.

As the Supreme Court recognized, “[a]s technology has enhanced the Government’s capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.” *Carpenter*, 138 S.Ct at 2214 (internal quotation marks and citations omitted). For the reasons stated above, the search and seizure of all electronic devices, which include cell phones, as a result of its mere presence inside a premises to be searched is no longer permissible post-*Riley*. The limitation on electronic device seizures in this warrant, however, protects the privacy interests of unrelated parties to the offense, ensures that the warrant satisfies the particularity requirement of the Fourth Amendment, and that the seizure is supported by probable cause. *See Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971) (“This particularity requirement protects person against the government’s indiscriminate rummaging through their

property.”).

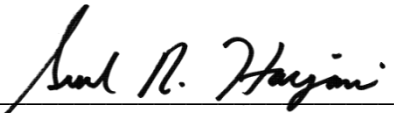
This is not to say that the government can never demonstrate that a seizure of all electronic devices is warranted. Situations, such as when the perpetrator of the offense lives alone or when probable cause demonstrates that all individuals in a premises were involved in an offense, could support a broader warrant for the seizure of all electronic devices. *See, e.g., United States v. Taylor*, 2019 WL 281547 at*8 (N.D. Cal. Jan 22, 2019) (warrant provided probable cause that both defendant and his wife were involved in tax fraud, and thus warrant for seizure of electronic devices was not overbroad). Like any warrant application, the government must provide specific probable cause to support a search and seizure for the items it seeks. The Court recognizes that there are challenges for law enforcement in identifying the specific devices within a residence that are connected to the offense or its perpetrator. However, these challenges can be overcome by law enforcement through the use of additional investigative techniques, such as pre-search surveillance focused on the devices used in the crime, dialing known phone numbers of the perpetrators while in the premises, or voluntary interviews of individuals present in the residence at the time of the search. And once the electronic devices subject to the warrant are seized, law enforcement is permitted to search the entirety of the device for evidence of the crime as described in the warrant. *United States v. Bishop*, 910 F.3d 335, 337 (7th Cir. 2018).

Conclusion

For the reasons stated above, the Court finds that the government's proposed search warrant satisfies the particularity requirement of the Fourth Amendment, and thus the Court grants the government's application for the warrant.

SO ORDERED.

Dated: April 20, 2020



Sunil R. Harjani
United States Magistrate Judge