UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

United States of America

v. Criminal No. 13-cr-98-JL
Opinion No. 2014 DNH 236P

Olawaseun Adekoya

MEMORANDUM ORDER

This case involves the warrantless seizure of an arrestee's cellular phone, and the subsequent use of information from the exterior of the phone in furtherance of an investigation. That arrestee, defendant Olawaseun Adekoya, was one of the targets of a sting operation that drew several of his acquaintances (but not Adekoya himself) to New Hampshire in order to purchase fraudulent ATM cards, which they intended to use to withdraw money from unknowing victims' bank accounts. The plan was foiled by federal agents, who arrested the participants in the act of attempting to withdraw cash with the cards.

Based upon information implicating Adekoya in the scheme, federal agents arrested him at his home in New Jersey the next day. During the arrest, the agents seized a cellular phone (precisely where the phone was located at that time, as will be discussed, is the subject of some debate between the parties). Later, using an identification number inscribed on the phone's exterior--known as an international mobile equipment identity, or "IMEI," number--the prosecution subpoenaed the phone's records,

which revealed that incriminating communications passed between that phone and phones seized from the New Hampshire arrestees at and around the time of the crime.

A jury in this court ultimately convicted Adekoya of bank fraud, in violation of 18 U.S.C. § 1344, and conspiracy to commit bank fraud, in violation of 18 U.S.C. §§ 371 & 1344. Prior to trial, Adekoya moved to suppress the phone, as well as the records that had been obtained using the IMEI, as fruits of an illegal search in violation of his Fourth Amendment rights. Adekoya's motion challenged both the seizure of the phone and the government's subsequent use of the IMEI number to obtain records from the service provider associated with the phone. Specifically, the motion argued:

- that the phone was not located in Adekoya's hand at the time of arrest, as the arresting agents claimed, but rather on a dining room table, outside of the space that permissibly can be searched by law enforcement incident to arrest, see Chimel v. California, 395 U.S. 752 (1969); and
- that even if the phone had been lawfully seized, the Fourth Amendment required the government to obtain a warrant before viewing the IMEI number.

The court held a hearing on the motion, at which several federal agents testified for the prosecution. Adekoya's father, who was present when his son was arrested, testified on Adekoya's behalf. The court then issued, on the record at the hearing, an oral order that (1) found that the phone had been in Adekoya's

hand at the time of arrest; (2) concluded that, because the phone was in Adekoya's hand, the arresting agents had lawfully seized it incident to arrest; and (3) concluded that the government needed no search warrant to view the IMEI number. The court accordingly denied Adekoya's motion, and now issues this written order to explain its findings and conclusions in more detail. See, e.g., United States v. Joubert, 980 F. Supp. 2d 53, 55 & n.1 (D.N.H. 2014) (noting a district court's authority to later reduce its prior findings and rulings to writing).

I. Background

Based upon the testimony and other evidence presented at the hearing, the court makes the following factual findings.

This case evolved out of an earlier investigation into a Vietnamese national, Hieu Minh Ngo, whom the United States Secret Service suspected of operating a website that sold substantial amounts of personally identifiable information ("PII"), including Social Security and driver's license numbers, that belonged to other individuals. Due to the lack of an extradition treaty between the United States and Vietnam, the Secret Service lured Ngo to the U.S. territory of Guam, arrested him, and transported him to New Hampshire to face charges in this court. Confronted with the prospect of a lengthy term of imprisonment, Ngo agreed

to cooperate with further investigations into individuals who had purchased PII from him, and authorized Secret Service Special Agent Matthew O'Neill to access and use his e-mail account.

Agent O'Neill, who is stationed in New Hampshire, discovered correspondence between Ngo and several e-mail accounts that originated from an IP address associated with Adekoya's New Jersey residence. In these exchanges, Ngo's correspondent sought to purchase several persons' Social Security numbers. Using this information, the government obtained an indictment against, and an arrest warrant for, Adekoya in this court.

Rather than having Adekoya arrested immediately upon the warrant's issuance, O'Neill took a different tack. Knowing that defendants in cases involving Internet communications frequently invoke the so-called "some other dude did it" or "SODDI" defense, and claim that someone else was behind the keyboard, O'Neill sought to lure Ngo's correspondent, who he believed to be Adekoya, to New Hampshire. In so doing, he hoped to demonstrate that Adekoya himself had corresponded with Ngo regarding the purchase of PII.

To this end, O'Neill, impersonating Ngo, wrote to one of the e-mail accounts that originated from the IP address associated with Adekoya's home, asking whether Ngo's correspondent would be interested in traveling to New Hampshire to engage in an "ATM

cashout," a scheme in which fraudulently manufactured ATM cards are used to withdraw funds from legitimate bank accounts. The user responded affirmatively, suggesting that he would be able to assemble a team of individuals to participate in the cashout. He and O'Neill, still in the virtual guise of Ngo, then proceeded to discuss the logistics of the scheme, the potential payout, the division of the proceeds, and various other details.

The scheme was put into action on October 1, 2013, when four individuals traveled from Atlanta, Georgia to Manchester, New Hampshire to conduct the cashout. As discussed by O'Neill and his correspondent, the four proceeded to a local hotel, where they retrieved a package containing 200 white plastic cards, which they had been led to believe were encoded to access ATMs, and several lists of banks in Manchester to be targeted. From there, they set out for the listed banks. After attempting to use the ATM cards during the early morning hours of October 2, all four individuals were arrested.

Although O'Neill, masquerading as Ngo, had insisted that he would deliver the cards to his correspondent only if the latter personally came to New Hampshire to pick them up, Adekoya was, to O'Neill's surprise, not among the four individuals arrested. Nonetheless, when law enforcement agents questioned the four, they indicated that one of them, Adebayo Adegbesan, had been in

contact via text messages with Adekoya, who resided in New Jersey. The arrestees also claimed that they had come to New Hampshire at Adekoya's request.

Following the events of October 2, O'Neill requested that inspectors of the United States Postal Inspection Service ("USPIS") in New Jersey execute the arrest warrant for Adekoya and take him into custody.[1] Thus, on the morning of October 3, 2013, a four-person team from the USPIS traveled to Adekoya's residence, where he lived with his parents, to arrest him.

The USPIS team waited outside the home for several hours, hoping to observe Adekoya either arriving or leaving, to no avail. When a delivery truck arrived at the residence, the team saw someone open the door to receive the package, but could not positively identify that person as Adekoya. At that point, they approached the residence and knocked on the door, which Adekoya opened. At the request of the USPIS inspectors, Adekoya stepped outside to speak with them, and was promptly arrested. When placing Adekoya in handcuffs, the arresting inspectors seized a cellular phone from his hand, which they then took with them.[2]

---

[1]The New Hampshire division of USPIS had also been involved in the investigation into Adekoya, and the New Jersey division of USPIS was already familiar with him from a previous investigation into similar alleged crimes.

[2]The court makes this finding based principally upon the testimony of two USPIS inspectors--Ketty Larco and Eric Malecki--

Several months after Adekoya's arrest, O'Neill subpoenaed the telephone records associated with the phone seized from Adekoya, identifying the phone by reference to the IMEI number inscribed on its back. Those records revealed a number of text messages between that phone and several of the phones seized from the four individuals arrested in New Hampshire, both on and leading up to the night of the attempted cashout.

---

at the suppression hearing. Inspector Larco testified that she took the phone from the defendant's hand herself when arresting him, while Inspector Malecki testified that Inspector Larco told him at the scene of the arrest that she had seized the phone from Adekoya's person (although he did not personally observe that). Adekoya's father gave contrary testimony at the suppression hearing, where he claimed that the phone was located on the dining room table during the arrest.

As discussed in detail on the record at the hearing, the court found the inspectors' testimony more consistent and more credible than the testimony of Adekoya's father. The inspectors had no strong incentive to give false testimony, as they had no involvement in the investigation apart from being asked to effectuate Adekoya's arrest. Their delivery, demeanor, and tone gave a credible impression; they did not appear to be attempting to shade or color their testimony in any way so as to advance the prosecution's position. Their accounts were consistent with one another and internally consistent, not to mention consistent with a jailhouse phone call made by the defendant (admitted into evidence at the hearing) in which he stated that "the phone was in my possession [and] they took it."

The defendant's father, by contrast, had an obvious motive to try to benefit his son. While it was clear to the court that the elder Adekoya was somewhat disappointed that his son had yet again found himself in trouble with the law, it was also apparent that he cared deeply for him. His testimony was disjointed and inconsistent, and his delivery, demeanor, and tone were defiant and indignant--a mien that is perhaps understandable given his son's predicament (and his own occupation as a New York City cabdriver), but which certainly did not enhance his credibility.

II. Analysis

As mentioned at the outset, Adekoya challenges both the USPIS inspectors' warrantless seizure of the cellular phone at the time of his arrest, and Agent O'Neill's later viewing of the IMEI number inscribed on the phone, also without a warrant. When, as here, a criminal defendant challenges a warrantless search or seizure, the prosecution bears the burden of showing, by a preponderance of the evidence, that an exception to the warrant requirement applies. See United States v. Matlock, 415 U.S. 164, 178 & n.14 (1974); United States v. Dickerson, 514 F.3d 60, 66 (1st Cir. 2008). For the reasons that follow, the prosecution has carried its burden here, and has demonstrated that both the seizure of the phone, and the subsequent viewing of the IMEI number, were permissible under recognized exceptions to the Fourth Amendment's warrant requirement. Adekoya's motion is accordingly denied.

A. Seizure of the phone

The Fourth Amendment to the U.S. Constitution protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV; see also Katz v. United States, 389 U.S. 347, 353 (1967). Generally, for a search or seizure of property

to qualify as "reasonable," law enforcement agents must first "secure a search warrant supported by probable cause." United States v. Gifford, 727 F.3d 92, 98 (1st Cir. 2013). Like many rules of general applicability, however, this one has exceptions. One of those is particularly relevant here: "[i]t is well settled that a search incident to a lawful arrest is a traditional exception to the warrant requirement of the Fourth Amendment." United States v. Robinson, 414 U.S. 218, 224 (1973).

That exception, succinctly summarized, "permits an arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction." United States v. Wurie, 728 F.3d 1, 3 (1st Cir. 2013), aff'd sub nom. Riley v. California, 134 S.Ct. 2473 (2014). As discussed in Part I, supra, the court finds that the phone in question was on Adekoya's person--specifically, in his hand--at the time he was arrested. It was, therefore, potentially fair game for seizure under the exception (to which the court will refer in the remainder of this order as the "search-incident exception").

The court's analysis cannot end there, however. Adekoya argues that even if the phone was, indeed, in his hand at the time of his arrest, the search-incident exception does not apply because neither of the twin aims of the exception--protecting the safety of arresting officers and preventing the destruction of

evidence--was implicated. He is incorrect as to both the facts and the law. USPIS Inspector Eric Malecki, who participated in the arrest, testified at the suppression hearing that Agent O'Neill had informed him prior to the arrest that Adekoya's alleged co-conspirators claimed to have been in phone contact with Adekoya during the commission of the cashout. So, as the court discussed on the record at the hearing, there was in fact good reason for the USPIS inspectors who arrested Adekoya to believe that evidence might exist on the phone (in the form of text messages or call history documenting Adekoya's exchanges with those who directly participated in the cashout) and that this evidence could be destroyed if the phone was not seized.

Even if one accepts Adekoya's position that neither aim was implicated, moreover, that still does not mean the seizure of the phone was unlawful. It is true that the Supreme Court, in articulating the search-incident exception, originally justified it as necessary to protect officer safety and to prevent the concealment or destruction of evidence. See Chimel, 395 U.S. at 763. The Court later explained, though, that while the exception is "based upon the need to disarm and to discover evidence," a search incident to a lawful arrest is reasonable 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, 414 U.S. at 235; see also Riley, 134 S.Ct. at 2485. So the USPIS inspectors' seizure of Akekoya's phone without a warrant at the time of his arrest was permissible under the Fourth Amendment, whether or not they had reason to believe their own safety was endangered or that evidence might be destroyed.

B. Viewing the IMEI number

Even when law enforcement agents permissibly seize a phone when making an arrest, they do not then have carte blanche to do whatever they wish with it. The Fourth Amendment's prohibition of unreasonable searches places at least one limitation on law enforcement's ability to examine a phone after a lawful seizure, preventing the viewing of the digital data stored on the phone without a warrant. See Riley, 134 S.Ct. at 2495 ("Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is . . . simple--get a warrant."). Adekoya asserts that a similar rule should govern law enforcement agents' viewing of the IMEI number on a cell phone. He maintains that if "a state actor had to manipulate the phone in any manner in order to view the IMEI number"--including simply turning the phone over to look at the back of it--"that action constitute[s] a search," prior to which the government must obtain a warrant. Deft.'s Reply (document no. 77) at 1.

Adekoya is incorrect, at least as far as the IMEI number in this case is concerned. The Supreme Court's recent decision in Riley reaffirmed that the search-incident exception entitles law enforcement officers to "examine the physical aspects of a phone" after seizing it. Riley, 134 S.Ct. at 2485; cf. also Wurie, 728 F.3d at 3 n.1 (suggesting that, once phone is lawfully seized incident to arrest, officers are "entitled to take notice of any information that [is] visible to them on the outside of the phone"). It is undisputed that the IMEI number on the phone seized from Adekoya was inscribed on the phone's rear exterior, and that no protective case enclosed the phone, so that the IMEI number was visible to the naked eye. As such, it falls easily within the category of the phone's "physical aspects" that are subject to examination without a warrant.

As the concurring opinion in Riley notes, moreover, "[i]t has long been accepted that" the search-incident exception permits the examination of "written items found on the person of an arrestee." 134 S.Ct. at 2496 & n.* (Alito, J., concurring). That includes information contained in, among other things, a defendant's diary, wallet, notebooks, and check books. See id. (citing, inter alia, Hill v. California, 401 U.S. 797 (1979) and Warden, Md. Penitentiary v. Hayden, 387 U.S. 294 (1967)). It stands to reason that if law enforcement officers may permissibly

view the written information contained in these types of materials without a warrant, the substantially less intrusive warrantless viewing of an IMEI number on the exterior of a phone--which reveals, in and of itself, no personal information about the person from whom it is seized, and serves only to identify the phone--is similarly permissible under the Fourth Amendment.[3]

As a last-ditch effort, Adekoya also argues that even if the search-incident exception would otherwise permit law enforcement officers to view an external IMEI number without a warrant, a warrant should nonetheless have been obtained to view the IMEI number here if, as the government claims, there was probable cause to believe the phone contained evidence. In other words, Adekoya takes the position that when law enforcement possesses sufficient probable cause to obtain a search warrant, it must obtain one even when doing so would not ordinarily be required.

---

[3]As discussed in Part I, supra, several months apparently passed between the date on which Adekoya was arrested and the phone was seized, and the date on which Agent O'Neill viewed the IMEI number in order to prepare a subpoena for the phone records. Adekoya has not argued--in either his written memoranda or at the suppression hearing--that this lengthy delay bears on whether the viewing of the IMEI number was "incident to" Adekoya's arrest, so the court need not address that issue. But cf. United States v. Chadwick, 433 U.S. 1, 15 (1977) (search of footlocker, seized at time of defendants' arrest, that occurred over an hour after the seizure and long after defendants were in custody, could not "be viewed as incidental to the arrest"), abrogated on other grounds by California v. Acevedo, 500 U.S. 565 (1991).

He has cited no authority for this proposition, however (in fact, at the suppression hearing, his counsel conceded that he had none), and the court is not aware of any. In the absence of such authority, the court must reject Adekoya's argument, which runs counter to the rationale for, and, indeed, the very existence of, the search-incident exception. See Wayne R. LaFave, Search and Seizure: A Treatise on the Fourth Amendment, Section 2 572 (5th ed. 2012) (noting, with regard to that exception, that "because the right to make the search flows automatically from the preceding arrest, there would be no issue to be decided by the magistrate concerning the search even if there were time to consult him").

In sum, under the search-incident exception, Agent O'Neill permissibly viewed the IMEI number on the phone while preparing the subpoena, and the phone records thereby obtained need not be suppressed.

III. Conclusion

For the foregoing reasons, the defendant's motion to suppress[4] is DENIED.

SO ORDERED.

[4]Document no. 64.

Joseph N. Laplante
United States District Judge

Dated: November 12, 2014

cc: Arnold H. Huftalen, Esq.
Theodore M. Lothstein, Esq.