No. 15-4111

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

UNITED STATES OF AMERICA,
***Plaintiff/Appellee*,**

v.

ALI SABOONCHI,
***Defendant/Appellant*.**

On Appeal from the United States District Court
for the District of Maryland, Southern Division
(The Honorable Paul W. Grimm)

BRIEF OF APPELLANT

JAMES WYDA
Federal Public Defender
District of Maryland

MEGHAN SKELTON
Appellate Attorney
6411 Ivy Lane, Suite 710
Greenbelt, MD 20770
(301) 344-0600

Counsel for Appellant

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes and Rules

15-4111

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff/Appellee,

v.

ALI SABOONCHI,
Defendant/Appellant.

On Appeal from the United States District Court
for the District of Maryland, Southern Division
(The Honorable Paul W. Grimm)

BRIEF OF APPELLANT

JURISDICTIONAL STATEMENT

The district court had jurisdiction under 18 U.S.C.§ 3231. That court entered final judgment on February 11, 2015. (JA 2898.) Ali Saboonchi filed a timely notice of appeal on February 24, 2015. (JA 2904.) This Court has jurisdiction under 28 U.S.C. § 1291 and 18 U.S.C. § 3742.

ISSUES PRESENTED

I. When Ali Saboonchi crossed the border into the United States, the government seized his digital media, including an iPhone and USB drive. Days later, without a warrant, government agents made a complete digital copy of all the data, then conducted a forensic search. Was the warrantless search unreasonable under the Fourth Amendment?

II. The government charged Mr. Saboonchi with "knowingly and willfully" violating the Iran trade embargo. He asked for a jury instruction requiring the government to prove that he knew what the embargo prohibited, but wilfully violated the embargo anyway. (JA 572). Did the district court err in instructing that jury that the government need not prove that Mr. Saboonchi was aware of the contents of the regulatory scheme?

STATEMENT OF THE CASE

A grand jury charged Ali Saboonchi with multiple counts of violating the Iran trade embargo, in violation of 50 U.S.C. §§ 1702, 1705 and 31 C.F.R. §§560.203, 560.204.[1] (JA 29-49.) A jury convicted him on all counts. He now appeals his conviction.

---

[1] The combination of statutes and regulations comprising the embargo is known as the International Emergency Economic Powers Act (IEEPA) and Iranian Transactions and Sanctions Regulations (ITSR).

A. When Mr. Saboonchi crossed the United States border, the government seized his digital media, then several days later, conducted a warrantless search of the data.

The FBI received a tip that, in the fall of 2010, someone named Ali made some inquiries about specialized technology that has industrial, medical, and military applications. (JA 226.) The FBI traced the phone number used in that inquiry to Ali Saboonchi. (JA 226.) A Homeland Security Investigations (HSI) special agent named Kelly Baird launched a criminal investigation into trade embargo violations and named Mr. Saboonchi as a "person of interest." She then entered Mr. Saboonchi's name into a database that the Department of Homeland Security and Customs and Border Patrol (CBP) officers use to screen individuals and determine their admissibility at the United States borders. (JA 337-38.) When she entered Mr. Saboonchi's name into the database, she had no information about whether Mr. Saboonchi planned to travel abroad.[2] (JA 226.) Knowing that she did not have probable cause for any search, she wanted to position herself to be able to exploit a potential coincidental border crossing. (JA 221.)

Several weeks later, during the evening of March 31, 2012, Agent Baird got a

[2] After entering his name into the database, Agent Baird subpoenaed FedEx records and learned that Mr. Saboonchi had shipped what appeared to be industrial goods to the United Arab Emirates despite having told the supplier that the product's end user was domestic. (JA 228.) This transaction happened about a year before Agent Baird entered Mr. Saboonchi's name into the database. (JA 228.)

phone call from CBP Officer Kenneth Burkhardt, who said that Mr. Saboonchi had arrived five minutes earlier at the Rainbow Bridge, a point of entry into the United States in Buffalo, New York.[3] (JA 169, 219.) Officer Burkhardt asked Agent Baird if she wanted anything particular done at the border, and she responded, "I just instructed that if there were any electronic media found, I would like it detained." (JA 221; *see also* JA 168.) She also asked the officer to send the devices to her in Baltimore.

When she made that request, Agent Baird had no idea if Mr. Saboonchi had any cell phones or other electronic media with him. (JA 248.) She did not tell Officer Burkhardt to ask any specific questions or do anything else unusual. (JA 225.) At the suppression hearing later, she explained that "I wanted to be able to look at the media pursuant to our border authority." (JA 221.) She further explained that she "wanted to see if there was evidence of export violations . . . any evidence of criminality." (JA 225-26.)

Officer Burkhardt seized the devices. He explained that the only reason he seized Mr. Saboonchi's cell phones and USB drive was because Agent Baird asked

---

[3] Border Patrol officers routinely query the database discussed above. In doing so on this occasion, the primary inspection officer found Agent Baird's entry and referred Mr. Saboonchi to secondary inspection. (JA 166-67.) Officer Burkhardt conducted the secondary inspection.

him to. (JA 168, 171, 212.) He did not know, and she did not tell him, why she wanted him to seize the devices, nor did she explain why she had entered Mr. Saboonchi's name into the database. (JA 207.)

He observed nothing independently at the border that would have prompted him to seize the devices or even take a cursory glance through the phones. (JA 187-89.) He in fact did not examine the contents of the phones or USB drive in any way. (JA 205.) Instead, right away, he gave the digital devices to a local Buffalo HSI agent.

Meanwhile, Officer Burkhardt asked Mr. Saboonchi "routine questions" and conducted a "routine" seven-point search of Mr. Saboonchi's car. (JA 156, 169.) The sole prompting for any of this questioning and searching was the database entry. (JA 186.) Officer Burkhardt found nothing of note in the car or on Mr. Saboonchi's person. (JA 169.) Agent Burkhardt learned that Mr. Saboonchi is a United States Citizen who had been visiting a college roommate in Buffalo. Mr. Saboonchi and his wife took a day trip to Niagara Falls. Everything about Mr. Saboonchi's trip struck Officer Burkhardt as "common" sightseeing; nothing seemed at all unusual. (JA 191.) They carried no large sums of cash and carried no contraband. (JA 171, 184.) Officer Burkhardt characterized his interaction with Mr. Saboonchi and his findings as "absolutely routine." (JA 175, 178.)

Two days later, Agent Baird received an email from an HSI agent in Buffalo that the two smart phones and USB drive were on their way to her in Baltimore via FedEx. (JA 222-23.) On April 4, 2012, she turned the devices over to a forensic examiner, who made a digital image of the devices. (JA 231.) She "took a look at" the data stored on the two smart phones and USB drive, then later reviewed the entire contents. (*Id.*) On April 13, 2012, she returned the two cell phones and the USB drive to Mr. Saboonchi, but retained all the data in the form of the digital images.[4] (JA 234.) She testified that she did not believe that she needed any reasonable suspicion of any unlawful activity in order to seize and conduct a forensic search of the digital media. (JA 242.)

B. The District Court rejected Mr. Saboonchi's proposed jury instruction that would have defined willfulness as knowingly and intentionally violating a known legal duty.

In his jury trial, Mr. Saboonchi contested few facts. For the most part, he agreed that the events that the government described actually occurred. He did not dispute that he had sent certain items to an intermediary country for transshipment to Iran. Nor did he dispute that the ITSR required a license to export the items. But he contested whether he knew about that licensing requirement. (JA 2789, 2792.) The

[4] Agent Baird testified that she eventually destroyed the digital image of the Sony Xperia, after reviewing the data from that phone, and deciding that it belonged to Mr. Saboonchi's wife.

crux of his defense was that he did not possess the specific intent *mens rea*.

The government proposed an instruction regarding the intent element that stated, "While the government must show that the defendant knew that his conduct was illegal, it is not necessary for the government to prove that the defendant had read, was aware of, or had consulted the specific regulations governing his activities. In other words, the government is not required to prove that the defendant read, was aware of, or had consulted the ITSR and the licensing requirements that those regulations describe." (JA 556.)

Mr. Saboonchi objected to this instruction, arguing that it was inconsistent with prevailing pattern instructions defining "knowingly" and "willfully," and that it eliminated the required finding that Mr. Saboonchi knowingly and intentionally violated a known legal duty. He also argued that this instruction misinterpreted the statute and regulations at issue. (JA 571.) He proposed the instruction: "To find that the defendant acted willfully, you must find beyond a reasonable doubt that he knew that his actions violated [the statute, regulations, and executive orders]." (JA 572.)

The district court denied Mr. Saboonchi's request. (JA 2358-64.) The final jury instruction stated, "While the government must show that the defendant knew that his conduct was unlawful, it is not necessary for the government to prove that the defendant had read or was aware of the contents of the [statute and regulations]." (JA

2631.) Thus, the instructions directly contradicted what Mr. Saboonchi had requested.

SUMMARY OF ARGUMENT

The warrantless search of all the data on Mr. Saboonchi's smart phones and USB drive was unreasonable under the Fourth Amendment. The border search exception does not excuse this warrantless search.

Riley v. California changes the way courts must analyze warrantless searches of data on smart phones. *Riley* held that cell phones, as a category, are different from other personal property subject to warrantless searches because of the vast quantity of profoundly personal and private data they contain. *Riley* did not overrule the warrant exception at issue (a search incident to arrest), but assigned different weights to the interests that courts must balance when examining warrantless searches. The balance tilts in favor of the individual's interests because of the quantity and nature of the information exposed in a data search, despite the heightened governmental interest.

Riley applies to this search. Like in *Riley*, the government has a heightened interest supporting warrantless searches at the border. But the individual's privacy interest in the data is identical. The Fourth Amendment balance therefore tilts in favor of the individual. Even if other border searches do not, searching data from a

cell phone requires a warrant.

In any event, under a more traditional border search analysis, this search was still unreasonable. The search exceeded the scope of a valid warrantless border search because it was not narrowly tailored to the justification for the exception. This search was untethered to the purposes behind the warrant exception. Moreover, it was unbounded by geography, scope, or duration. It began four days after Mr. Saboonchi crossed the border, took place 350 miles from where he crossed, lasted indefinitely, and assisted by technology, intruded comprehensively and deeply into a privacy interest that the Supreme Court has equated with the privacy enshrined in a home.

The district court also erred in refusing Mr. Saboonchi's requested jury instruction defining willfulness. When the government charges a crime based on complex regulatory schemes, like the Iran Trade Sanctions Regulations, it must prove that the defendant knew what the law stated, and knowingly and intentionally violated that known legal duty. Here, the court instructed the jury that it could convict Mr. Saboonchi if it decided that he knew, in general, that his conduct was unlawful. This instruction impermissibly watered down the intent element of the offense. It prejudiced Mr. Saboonchi because his entire defense was directed at intent. He did not deny the conduct; he denied knowing what the embargo prohibited and that he

chose to violate the embargo.

STANDARD OF REVIEW

Whether a search is reasonable under the Fourth Amendment is a question of law that this Court reviews *de novo*. *United States v. Breza*, 308 F.3d 430, 433 (4th Cir. 2002).

This Court reviews the denial of a defendant's requested jury instruction for abuse of discretion. *United States v. Sonmez*, 777 F.3d 684, 688 (4th Cir. 2015). To establish an abuse of discretion, the defendant must demonstrate that the proposed instruction (1) was correct; (2) was not otherwise covered by the instructions that the district court actually gave to the jury; and (3) failing to give the instruction impeded the defense. *Id.*

ARGUMENT

I. The warrantless search of data contained in Ali Saboonchi's smart phones and USB drive violated the Fourth Amendment.

A Border Patrol officer seized Ali Saboonchi's iPhone 4S, his wife's Sony Xperia smart phone, and a USB drive at the Rainbow Bridge in Buffalo, New York, when Mr. Saboonchi was returning from a sightseeing day trip to Niagara Falls. The officer did not search or inspect the contents of the devices at the border. Several days later, a different agent shipped the devices to Baltimore, where a computer

forensics expert produced a complete digital image of the devices, then examined all the data.

Nothing that occurred at the Rainbow bridge, nothing about Mr. Saboonchi's trip, and nothing found on Mr. Saboonchi's person or in his car at the border prompted the seizure or subsequent warrantless search of his data. (JA 171, 186-89, 191, 212.) Instead, government agents decided to conduct the sweeping search of his data weeks earlier, when they entered his name into a database that prompts warrantless border searches, although the agents did not even know if Mr. Saboonchi, a United States citizen, had any plans to travel abroad. (JA 226-28.) By entering Mr. Saboonchi's name into the database, government agents hoped to position themselves to exploit the border search doctrine, knowing they did not have probable cause, to investigate what they believed might have been past criminal conduct.

For multiple overlapping reasons, the warrantless search of Mr. Saboonchi's data violated the Fourth Amendment.[5] Although the government enjoys broad authority to conduct warrantless searches at the border, that power is not absolute. An individual's privacy interest in data – especially the quantity and quality of data contained on a smart phone – outweighs the government interest in conducting

[5] The Fourth Amendment states that "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."

warrantless border searches. The highly intrusive nature of the search also impacts the constitutional balance in favor of the individual's privacy interests. The Fourth Amendment therefore requires a warrant based on probable cause in order to perform the search that occurred here. Anything less is constitutionally unreasonable.

Moreover, the search exceeded the scope of a valid warrantless border search. It was a general rummaging for evidence of a past crime, unrelated to the purposes giving rise to the border exception. The breadth and duration of the search far exceeds any border search that the Supreme Court has ever approved.

A. Balancing the extensive intrusion into an individual's substantial privacy interest against the government's interests at the border, the Fourth Amendment requires a warrant supported by probable cause for this search.

To assess whether a search is reasonable, courts balance the intrusion into an individual's Fourth Amendment interests against the legitimate governmental interest at stake. *United States v. Montoya de Hernandez*, 473 U.S. 531, 539 (1985). *See also Riley v. California*, 134 S. Ct. 2473, 2484 (2014) ("We generally determine whether to exempt a given search from the warrant requirement by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.") (internal quotation omitted). "What is reasonable depends upon all of the

circumstances surrounding the search or seizure and the nature of the search or seizure itself." *Montoya de Hernandez*, 473 U.S. at 537.

1. An individual's privacy interest in data stored in and accessible through a cell phone is extensive.

"Modern cell phones, as a category, implicate privacy concerns far beyond those implicated" by searches of other property someone may carry on his or her person. *Riley*, 134 S. Ct. at 2488. "Cell phones differ in both a quantitative and a qualitative sense from other objects." *Id.* at 2489.

a. Quantity

An individual's privacy interest in cell phone data is substantial simply because of the sheer quantity of information. A person's ability to carry around physical photographs, mail, videos, bank records, books and newspapers is necessarily limited, but the storage capacity of smart phones makes the impossible possible. An iPhone like Mr. Saboonchi's allows a person to carry the equivalent of thousands of photographs, songs, videos, and/or *millions* of pages of text.

These privacy interests are constantly growing because of technological advances improving both storage and functionality of cell phones.[6] The "gulf

[6] For example, Mr. Saboonchi owned the fifth generation of iPhone. Since his model first became available to consumers, Apple has introduced three more versions of iPhone, and is expected to introduce another on September 9, 2015.

between physical practicability and digital capacity will only continue to widen in the future." *Riley*, 134 S. Ct. at 2489. This Court recognizes that it must "take such developments into account" when assessing the constitutionality of a particular search. *United States v. Graham*, __ F.3d __, 2015 WL 4637931 at *13 (4th Cir. 2015). "The Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish." *United States v. Warshak*, 631 F.3d 266, 285 (6th Cir. 2011).

b. Quality

The type of data stored on and accessible from cell phones also implicates a substantial privacy interest. As the district court explained, a forensic search of digital media reveals "a class of data that raises novel privacy concerns, including files that a user had marked as 'deleted' and location data that may provide information about activities in the home and away from the border." (JA 349.)

"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." *Riley*, 134 S. Ct. at 2489. Data that does not exist in the physical world exists on cell phones. Internet search history, historic location information, and apps that manage "detailed information" about a person's plans, interests, activities, and goals, "form a revealing montage of the user's life."

Id. at 2490. As a result, "the sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions." *Id.* The data that the government can extract from cell phones "can reveal both a comprehensive view and specific details of the individual's daily life." *Graham*, 2015 WL 4637931 at *11. The search here "enables the government to ascertain, more or less at will, private facts about the individual, such as her 'political and religious beliefs, sexual habits, and so on.'" *Id.* at *10 (quoting *United States v. Jones*, 132 S. Ct. 945, 956 (2012) (Sotomayor, concurring)).

Smart phones, like Mr. Saboonchi's, provide access to data that is not even stored on the phone itself. *Riley*, 134 S. Ct. at 2491. Because of cell phones' ability to take advantage of cloud computing, a search of a cell phone enables the government to examine information "stored in remote servers rather than on the device itself." *Id.* The search thus defies physical boundaries.

As the district court noted, cell phones also contain location data, something *Riley*, as well as this Court, noted is particularly private and sensitive. *Riley*, 134 S. Ct. at 2490; *Graham*, 2015 WL 4637931 at *8. "Examination of a person's historical [location data] can enable to government to trace the movements of the cell phone and its user across public and private spaces and thereby discovery the private activities and personal habits of the user. Cell phone users have an objectively

reasonable expectation of privacy in this information." *Id.*

The Supreme Court described the privacy interest in cell phone data as even greater than the privacy interest in a home, which enjoys the highest Fourth Amendment protection. The Court explained that searching a cell phone, is "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." *Riley*, 134 S. Ct. at 2491 (emphasis in original).

The search exposes not just the contents of particular files, but information *about* the files, which reveals a whole new category of private details. For example, a search of a physical photograph reveals only a static image. But searching a digital file of an image can reveal when and where it was taken, if it was shared with anyone, personally identifying information about the people to whom it was sent, how it was sent, and if it was edited or deleted.

Moreover, the intrusive nature of the search itself highlights the individual's privacy interest. "A search of the information on a cell phone bears little resemblance to" a "physical search." *Riley*, 134 S. Ct. at 2485. The district court described the exhaustive search that occurred here. Searching data on a smart phone begins with creating a perfect image or copy of the contents of the original device. (JA 348.)

Then a computer forensics expert uses "specialized software to comb through the data, often over the course of days, weeks, or even months, searching the full contents of the imaged hard drive, examining the properties of individual files, and probing the device's unallocated 'slack space' to reveal deleted files." (JA 348.) The process, assisted by technology, "searches vast amounts of data that would exceed the capacity of a human reviewer to examine in any reasonable amount of time." *Id.* *See also* *United States v. Cotterman*, 709 F.3d 952, 962 (9th Cir. 2013) (describing the "comprehensive and intrusive" forensic examination of a laptop).

A manual search of data cannot compare to a forensic search: "No matter how thorough or highly motivated the agent is, a manual search of a computer or digital device will never result in the human visualization of more than a fraction of the content of the device." (JA 349.) In contrast, the information available to the government after conducting a "sophisticated, technology-assisted" search vastly exceeds what is visible to the unassisted human examiner.

This degree of invasion into a Fourth Amendment privacy interest necessarily impacts the factors courts must balance. *See Graham*, 2015 WL 4637931 at *12 ("The Fourth Amendment challenge is directed toward the government's investigative conduct."). The government may not exploit evolving technology in a manner that "erodes the privacy guaranteed by the Fourth Amendment." *Kyllo v. United States*,

533 U.S. 27, 34 (2001). Thus, the fact that the search was a comprehensive examination of all the phone's data and metadata, rather than a cursory glance at a few text messages is relevant to the Fourth Amendment balance. While a quick glance may not infringe upon the same level of privacy interests, the type of search here involved the maximum intrusion.

Cell phones contain "the privacies of life." *Riley*, 134 S. Ct.. at 2495. Smart phones, and all of us who use them, deserve the highest Fourth Amendment protections.

2. The government's interest in protecting the integrity of the border is also substantial.

To be sure, the government has broad powers to advance "the government's interest in preventing the entry of unwanted persons and effects . . . at the international border." *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004). The government has a particularly strong interest in enforcing customs duties, preventing smuggling, and preventing inadmissible people or contraband from entering the country. *United States v. Ramsey*, 431 U.S. 606, 620 (1977).

"Travelers may be stopped in crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which may lawfully be

brought in." *Carroll v. United States*, 267 U.S. 132, 154 (1925). The border search exception to the Fourth Amendment's warrant requirement "is grounded in the recognized right of the sovereign to control, subject to substantive limitations imposed by the Constitution, who and what may enter the country." *Ramsey*, 431 U.S. at 620.

Although the government has a heightened interest in preventing smuggling and excluding contraband or inadmissible individuals and items from entering the country, not every warrantless border search is automatically reasonable. The border search exception does not confer "unfettered discretion" on law enforcement. *Almeida-Sanchez v. United States*, 413 U.S. 266, 272-73 (1973). People who present themselves at the border are still "entitled to be free from unreasonable searches and seizures." *Montoya de Hernandez*, 473 U.S. at 539.

3. When it comes to searching cell phone data, *Riley* fundamentally alters the balance between the government's interest and the individual's Fourth Amendment rights.

Riley fundamentally changes the balance of Fourth Amendment interests when the government is searching the data on a cell phone. Courts cannot ignore the nature of cell phones and existing (and evolving) technology while mechanically applying legal principles that developed when a smart phone like Mr. Saboonchi's (or the *Riley* defendants') "were unheard of." *Riley*, 134 S. Ct. at 2484. *Riley* held that to treat a

cell phone search as "materially indistinguishable" from a search of any other personal property is absurd. *Id.* at 2488 ("That is like saying a ride on horseback is materially indistinguishable from a flight to the moon.")

Riley is not limited to searches incident to arrest. The decision unequivocally addresses cell phones "*as a category*." *Id.* at 2488 (emphasis added). Rather than questioning the governmental interests at stake or the assumptions underlying the warrant exception, the Court re-focused the analysis on the numerous ways that the quality and quantity of data on a cell phone change the weight of the Fourth Amendment interests that courts must balance.

Riley's analytical framework applies to any warrant exception. The search incident to arrest does not involve its own unique balancing test. It uses the same balance that applies whenever a court considers any exception to the warrant requirement. It compared the traditionally diminished individual expectation of privacy with the heightened governmental interest during an arrest. *Id.* at 2485. The Court acknowledged the government's weighty interest when searching someone incident to arrest. But considering the competing individual privacy interest in cell phone data, the balance tips toward the defendant.

Riley establishes that searches of data are simply different. Certainly the principles underlying both border searches and searches incident to arrest still exist.

Riley did not eliminate the search-incident-to-arrest exception, and Mr. Saboonchi does not argue that all warrantless border searches are unreasonable. Nevertheless, *Riley* clarifies that courts cannot apply the same old analysis of traditional warrant exceptions. When it comes to searching cell phone data, a court can no longer simply recite the mantra that individuals have a diminished privacy interest at the border (or when being arrested) versus the government's heightened interest. The privacy implications of this new technology and the government's ability to infiltrate every aspect of an individual's daily life did not exist even a few years ago, let alone when the exceptions first developed. *Riley* recognized that the world has changed and that those changes cannot be divorced from the Fourth Amendment balance.

Riley controls the decision here. The search incident to arrest exception and border search exception involve comparable interests. *Ramsey* described the border search exception as "like the similar 'search incident to arrest' exception." 431 U.S. at 621 (citing *United States v. Robinson*, 414 U.S. 218, 224 (1973)). Both exceptions are grounded in a heightened governmental interest weighed against an individual's diminished expectation of privacy. *Compare Riley*, 134 S. Ct. at 2488 *with Montoya de Hernandez*, 473 U.S. at 539. Neither exception grants absolute, controlling weight to the government interest or scrubs the individual's interest to almost nothing. *Montoya de Hernandez*, 473 U.S. at 539; *see also Riley*, 134 S. Ct. at 2484-85

(describing the evolution of the search incident to arrest exception and its assumption that the arrestee has a reduced expectation of privacy).

The fact that a person has a diminished privacy interest "does not mean that the Fourth Amendment falls out of the picture entirely" *Riley*, 134 S. Ct. at 2488. "To the contrary, when 'privacy related concerns are weighty enough' a 'search may require a warrant, notwithstanding the diminished expectations of privacy.'" *Id.* (quoting *Maryland v. King*, 133 S. Ct. 1958, 1979 (2013)). *Riley* establishes that the privacy interest here is "weighty enough."

Mr. Saboonchi's privacy interests are identical to those in *Riley*. And the government's interests are highly analogous. Balancing the individual's privacy interest against the heightened governmental interest tilts decidedly in favor of requiring a warrant supported by probable cause. Just as in *Riley*, nothing prevents the government from seizing the phone at the border, securing it, then applying for a search warrant.

B. Because this search was the equivalent of an exhaustive search of a home, it exceeded the scope of a border search.

Because this search was as intrusive as searching a home, the Fourth Amendment requires a warrant. The border search exception does not apply to the equivalent of searching a home.

In *Ramsey*, the Court contemplated a border search that "might be deemed unreasonable because of the particularly offensive manner in which it is carried out." 431 U.S. at 618 n.13. One of the examples the Court cited involved the seizure and removal of the entire contents of a secluded cabin from a remote area in the Sierra Nevada mountains for an exhaustive search at the FBI offices 200 miles away. *Kremen v. United States*, 353 U.S. 346, 347-48 (1957). The Court's second example involved the warrantless "and apparently unlimited search, ransacking the desk, safe, filing cases, and other parts of the office." *Go-Bart Importing Co. v. United States*, 282 U.S. 344, 358 (1931). Thus, the limitless ransacking and rummaging through the entire contents of an office or residence is so "particularly offensive" in manner and scope as to exemplify what constitutes an unreasonable border search. *Ramsey*, 431 U.S. at 618 n.13. *See also Chimel v. California*, 395 U.S. 752 (1969) (holding that the extensive search of an arrestee's home exceeded the scope of a search incident to arrest).

And as *Riley* explains, the search that occurred here was tantamount to a comprehensive search of Mr. Saboonchi's home, office, and even metadata that is too hidden to independently exist in a home or office "unless the phone is." *Riley*, 134 S. Ct. at 2491. Yet these are the exact types searches that *Ramsey* identified as too "offensive" to qualify as a valid warrantless border search. 416 U.S. at 618.

The search of Mr. Saboonchi's data was strikingly similar to both of *Ramsey's* examples. The government shipped his data hundreds of miles away to dissect at its leisure. That data is essentially indistinguishable from what is kept in file cabinets and desks. Moreover, the search here had an even more expansive scope than the "particularly offensive" examples in *Ramsey* because, unlike those searches, this search was not limited by time or human perception. No byte of data or metadata was left unturned. The wholesale rummaging through Mr. Saboonchi's data exceeds the scope of a valid border search.

Not only was the search comparable to searching a home because of the type of information available from cell phones, but the search in fact allows the government to look inside a person's home. Discussing historic cell site location information, this Court stated that searching cell phone data "can allow the government to place an individual and her personal property – specifically, her cell phone – at the person's home and other private locations as specific points in time." *Graham*, 2015 WL 4637931 *9. But "'In the home, . . . *all* details are intimate details, because the entire area is held safe from prying government eyes.'" *Id.* (quoting *Kyllo v. United States*, 533 U.S. 27, 37 (2001) (ellipses and emphasis in *Graham*)). When the government searches a cell phone, it sees "critical private detail[s]" – the location of a person and personal property within a home at a specific

time – that the Fourth Amendment "protect[s] from the government's intrusive use of technology." *Id.*

Since this search allows to government to see the equivalent to the contents of Mr. Saboonchi's home and, more importantly, to learn specific details about his home, activities there, and when he and others are present, the government must get a warrant.

C. Other considerations also demonstrate that this search exceeded the scope of a valid warrantless border search.

1. Searches pursuant to warrant exceptions must be narrowly tailored to a specific goal.

Warrantless searches based on historically recognized warrant exceptions are reasonable when they are narrowly tailored to the purposes that gave rise to the pertinent exception. *See Arizona v. Gant*, 556 U.S. 332, 339 (2009) ("The scope of a search incident to arrest is commensurate with its purposes of protecting the arresting officers and safeguarding any evidence of the offense of arrest."). When the "justifications for the . . . exception are absent . . . the rule does not apply." *Id.*[7]

[7] *See also Terry v. Ohio*, 392 U.S. 1, 28-29 (1968) ("evidence may not be introduced if it was discovered by means of a seizure and search which were not reasonable related in scope to the justification for the initiation."); *Minnesota v. Dickerson*, 508 U.S. 336, 373, 378 (1993) (holding that a *Terry* frisk was unreasonable because the officer continued exploring the suspect's pockets after concluding that the suspect was not armed, meaning that the search was unrelated to the sole justification for the search); *Segura v. United States*, 468 U.S. 796, 823

Therefore, for the border search exception to apply, the search must be narrowly tailored to the purposes behind the exception, which is to allow "the sovereign to control, subject to substantive limitations imposed by the Constitution, who and what may enter the country." *Ramsey*, 431 U.S. at 620. The Constitution recognizes the exception "because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongs as effects which may be lawfully brought in." *Carroll v. United States*, 267 U.S. 132, 154 (1925). Thus, the exception applies when the search is targeted at "the sovereign's right and need to protect its territorial integrity and national security." *United States v. Kim*, __ F. Supp. 2d __ 2015 WL 2148070 *19 (D.D.C. 2015).

A search that is not linked to preventing inadmissible items, people, or contraband into the country, or collecting taxes, exceeds the scope of the exception. "The border search exception allows for warrantless, suspicionless searches and thus its application must remain tethered to its primary purpose." *United States v. Humphries*, 308 Fed. Appx. 892, 896 n.1 (6th Cir. 2009).

The only border searches that the Supreme Court has ever approved were

---

(1984) ("While exigent circumstances may justify police conduct that would otherwise be unreasonable if undertaken without a warrant, such conduct must be 'strictly circumscribed by the exigencies which justify its initiation.'" (quoting *Terry*, 392 U.S. at 25-26)); *United States v. Camou*, 773 F.3d 932, 940 (9th Cir. 2014).

specifically targeted at finding or preventing the entry into the United States of contraband or inadmissible persons.[8] Likewise, in the last twenty years, this Court has only approved border searches that are specifically targeted at the exception's purposes.[9] The only border searches that the Supreme Court or this Court have approved occurred because of events that unfolded at the border,[10] note because of law enforcement decisions made weeks before the crossing.

Even searches targeted at these goals only qualify for the warrant exception when they occur at the border (or its functional equivalent). The exception applies to "threats posed at the point of entry." *Kim*, 2015 WL 2148070 *19. In contrast, for

---

[8] *Carroll,* 267 U.S. 132 (importing alcohol during Prohibition); *Ramsey*, 431 U.S. 606 (narcotics concealed in letters); *United States v. 12 200-Foot Reels of Super 8mm Film*, 413 U.S. 123, 125 (1973) (obscenity); *United States v. Martinez-Fuerte*, 428 U.S. 543 (1976) (illegal aliens); *United States v. Cortez*, 449 U.S. 411 (1981) (illegal aliens); *Montoya de Hernandez*, 473 U.S. 531 (narcotics in an alimentary canal); *Flores-Montano*, 541 U.S. 149 (narcotics concealed in a vehicle driving across the border).

[9] *United States v. Taylor*, 584 Fed. Appx. 47 (4th Cir. 2014) (currency smuggling); *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005) (contraband child pornography); *United States v. Kaczmarak*, 62 Fed. Appx. 510 (4th Cir. 2003) (inadmissible alien); *United States v. Switzer*, 11 Fed. Appx. 65 (4th Cir. 2001) (drug smuggling); *United States v. Spence*, 199 F.3d 1329 (4th Cir. 1999) (currency smuggling); *United States v. Aguebor*, 166 F.3d 1210 (4th Cir. 1999) (alimentary canal heroin smuggler); *United States v. Aragon*, 155 F.3d 561 (4th Cir. 1998) (cocaine smuggling); *United States v. Oriakhi*, 57 F.3d 1290 (4th Cir. 1995) (currency smuggling).

[10] *See* cases cited in notes 8 and 9.

example, a search near the border but well inside the United States, although targeted at preventing the smuggling of undocumented aliens is nevertheless unreasonable. *Almeida-Sanchez v. United States*, 413 U.S. 266, 269-70 (1973).[11] The government enjoys "plenary authority to conduct routine searches and seizures *at the border*, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country." *Montoya de Hernandez*, 473 U.S. at 537 (emphasis added); *see also Carroll*, 267 U.S. at 132 (discussing searches at "an international boundary").

2. This search bore no relationship to the justifications for the border search exception.

The search of Mr. Saboonchi's data was wholly untethered to the purposes justifying warrantless border searches. It bore no relationship to preventing smuggling or excluding contraband.

This search was designed to uncover evidence of a past crime, not to protect the integrity of the border. Agent Baird entered Mr. Saboonchi's name into the database at the very earliest stages of an investigation, when she decided that he might be a "person of interest" to a possible crime that had occurred about a year

[11] Despite a statute authorizing CBP to conduct "roving patrols" "within a reasonable distance from any external boundary of the United States, the Supreme Court deemed this "extravagant license to search" unreasonable because it conferred "unfettered discretion on the members of the Border Patrol" *Id.* at 268, 270.

earlier. Knowing that CBP officers routinely query this database when checking passports, Agent Baird positioned herself to take advantage of the border search exception—just in case Mr. Saboonchi traveled abroad. The government thus decided to execute this search weeks before Mr. Saboonchi ever crossed the border. (JA 166-67, 226.)

Moreover, nothing that happened at or near the border provided any reason for search his data. The only reason the CBP agent who first encountered Mr. Saboonchi referred him for secondary inspection was this database hit. Nothing about his travel, his documents, his car – anything – prompted the secondary inspection. (JA 168, 171, 212, 221, 227.) The officer who conducted the secondary inspection testified that the only reason he seized the devices was because Agent Baird in Baltimore asked him to. (JA 168, 171, 212.) He testified that everything about Mr. Saboonchi's day trip to the Canadian side of Niagara Falls, the personal effects that he carried with him, the condition of his car, and the way he answered questions was "absolutely routine." (JA 175, 178.)

Here, unlike any of the border searches approved by the Supreme Court or this Court, there was no question of attempting to exclude inadmissible travelers, interdicting contraband, or preventing smuggling at the border. This was an expansive search, based on discretionary law-enforcement decisions for developing

a criminal case for litigation. As such, it was not a border search. *See United States v. Brennan*, 538 F.2d 711, 716 (5th Cir. 1976). The search of Mr. Saboonchi's data "was so particularized to the suspicions of the defendant's activities" that it "did not possess the characteristics of a border search or other regular inspection procedure. It more resembled the common non-border search based upon individualized suspicion, which must be prefaced by the usual warrant and probable cause standard." *Id.*

Comparing this search to other searches of digital media justified under the border search doctrine reveals that this search stands apart, devoid of any connection to excluding contraband. First, the search at issue in this Court's decision in *Ickes* shows numerous connections to protecting the border from contraband. Border Patrol officers found marijuana, drug paraphernalia, and a number of photographs of nude or near nude children. 393 F.3d at 503.[12] Similarly, in *Cotterman*, the Ninth Circuit

[12] Although this Court approved the warrantless search of digital media in *Ickes*, the case does not compel the same result here. In addition to the factual distinctions addressed above, the legal reasoning is no longer applicable. When that decision was issued in 2004, the digital world was nothing like it is today. It predated the first iPhone by three and a half years. Even more important, it predated *Riley* by ten years. *Ickes* rests on the assumption that it is "far fetched" to believe that customs agents could search the entire contents of every computer crossing the border. *Id.* at 507. Now, we know that is anything but far fetched. Moreover, the primary issue in *Ickes* was whether the First Amendment exempted "expressive materials" from the border search exception. 393 F.3d at 505-06. That issue is not present here.

identified numerous facts that were related to excluding child pornography: a database hit identifying the defendant as a sex offender,[13] an unusual number of cameras, frequent international travel, travel from a known sex-tourism destination, and an initial inspection of the digital media that showed password protected files. 709 F.3d at 968-69.

This search, on the other hand, was a classic search for evidence in an ongoing criminal investigation. This premeditated warrantless search was to find evidence to build the government's case and to use in a prosecution. "Where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing . . . reasonableness generally requires the obtaining of a judicial warrant." *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995). *See also Florida v. Wells*, 495 U.S. 1, 4 (1990) (explaining that an inventory search "must not be a ruse for a general rummaging in order to discover incriminating evidence" and that police officers "must not be allowed so much latitude that inventory searches are turned into a purposeful and general means of discovering evidence of a crime.") (internal quotation omitted)); *New York v. Burger*, 482 U.S. 691, 724 (1987) (explaining that probable cause is not required in most administrative searches, like border searches,

[13] In contrast, here, the CBP officer had no idea why Mr. Saboonchi's name was in the database.

because they are undertaken primarily for administrative rather than prosecutorial purposes) (citing *Almeida-Sanchez*, 413 U.S. at 278). This general rummaging for evidence in an ongoing criminal investigation falls outside the confines of a border search.

3. The time and place of this search also establish that the search was too attenuated from the purposes of the exception to render the warrantless search reasonable.

The search was not narrowly tailored to the purposes of the exception because neither time nor geography limited this search to the border search doctrine. This search did not occur at the border or its functional equivalent, or even at the time of the crossing.

Although the seizure occurred at the border,[14] the government did not search the digital devices there. The CBP officer made no effort to search the devices or even give a cursory glance at the contents of the phone. Instead, two days after seizing Mr. Saboonchi's digital devices, a government agent shipped them 350 miles

[14] The fact that government "agents were lawfully in possession" of the digital media "did not give them authority to search their contents." *Walter v. United States*, 447 U.S. 649, 654 (1980). "Ever since 1878 . . . it has been settled that an officer's authority to possess a package is distinct form his authority to examine its contents." *Id.* Even if the initial seizure of the devices was reasonable, the subsequent search must still stand on its own constitutional footing.

away from the border.[15] (JA 222-23.) Four days after Mr. Saboonchi presented himself at the border, and 350 miles away from where he crossed, the government finally began searching his data.[16] (JA 231.)

There was no question about Mr. Saboonchi's or his phone's admissibility into the United States. As a United States citizen, the government's choices were either to admit him, which it did, or arrest him. And his personal property was not

---

[15] This is analogous to *United States v. Place*, 660 F.2d 44, 50-52 (2d Cir. 1981), *affirmed by* 462 U.S. 696 (1983), where the Second Circuit held that transporting luggage from LaGuardia to JFK, on the basis of reasonable suspicion, in order to present the baggage to a drug-sniffing dog violated the Fourth Amendment. "If the agents had, on the basis of reasonable suspicion but without probable cause, merely exposed [the] baggage to a trained sniffer as he was passing through LaGuardia, this brief detention might, assuming reasonable grounds for suspicion, fall within the limits of *Terry* and its progeny." *Id.* at 51-52. Not so when the government seized the suitcase and moved it ten to fifteen miles between airports. *Id.* Instead, seizing the property, moving it to another location, and keeping it for several hours was an unreasonable search and seizure, "not unlike the use of Writs of Assistance which led to the adoption of the Fourth Amendment." *Id.* at 52. *See also Kremen*, 353 U.S. at 347 (transporting the property in a mountain cabin to FBI offices 200 miles away "for the purpose of examination [is] beyond the sanction of any of our cases.")

[16] Again, comparing this search to those in *Ickes* and *Cotterman* is telling. Those searches occurred geographically and temporally at the border crossing, because of events observed at the border. *See Ickes*, 393 F.3d at 503; *Cotterman*, 709 F.3d at 968-69. Although the forensic examination of the data occurred later, the cases involved an initial inspection of the digital media, prompted by circumstances that demonstrated a need to protect against the importation of contraband. The threat to the sovereign's integrity was acute at the point of entry, and the warrantless searches began immediately to defuse that threat.

contraband and obviously posed no danger to the interests that the border search exception protects, as the government itself brought the smart phones deep inside the country's boundaries.[17] It was the same property in essentially the same condition that he lawfully possessed when he left his home in Maryland.

Moreover, the nature of a forensic search of data means that the search has no temporal restrictions. After the government makes its complete digital copy of the data, it continues to search for days, weeks, and months, long after the person and property have returned to normal life within the nation's boundaries.

Even the most intrusive border searches that the Supreme Court has approved so far has been necessarily limited in time. In *Flores-Montano*, where the Court approved the removal and disassembly of a fuel tank, the secondary inspection took less than an hour. 541 U.S. at 151. In *Montoya de Hernandez*, the Supreme Court described the 16-hour detention as "undoubtedly exceed[ing] any other detention we have approved under reasonable suspicion." 473 U.S. at 543. But even as the hours

---

[17] The seizure and subsequent search here is not a situation where goods are detained, then inspected by customs officers, then ultimately released for importation. Some times, merchandise being imported might be detained and subjected to testing in order to determine admissibility or if a particular tariff applies. This applies to "merchandise in a commercial sense, to the exclusion of baggage, personal effects, and articles of personal adornment." *United States v. Mattio*, 17 F.2d 879, 880 (9th Cir. 1927). *See also Furie Operating Alaska, LLC v. Department of Homeland Security*, 2014 WL 1289581 (D. Ala. 2014); *Poland Bros. Inc. v. United States*, 64 Cust. ct. 248, 253, 1970 WL 14611 *5 (Cust. Ct. 1970).

ticked by, the government eventually sought and received a search warrant. *Id.* at 535.

If the Court were to assume that the search was complete when Agent Baird returned the digital devices to Mr. Saboonchi, the "border" search still would have taken two weeks. So far, sixteen hours has been the outer limit of the duration of a seizure at the border. At its most conservative estimate, this search took 336 hours. In reality, of course, the government retained the image for further study. This border search became indefinite. Warrantless searches cannot lost so long.

Rummaging through data on the off chance that evidence of a past crime might turn up is not a valid border search. This search was so attenuated from the justifications for permitting warrantless searches at the border – by purpose, location, duration, and scope – that the exception does not apply here.

D. If this Court decides that the Fourth Amendment requires only reasonable suspicion, the search is still unreasonable because the district court misapplied that standard here.

If this Court decides that reasonable suspicion is sufficient to justify warrantless searches of data after a seizure at the border, the search here still violated the Fourth Amendment. There was no reasonable suspicion that the search would reveal contraband or anything related to crime at the border. The facts known to the border patrol officer did not amount to reasonable suspicion.

1. When reasonable suspicion supports warrantless "non-routine" border searches, the suspicion must arise at the border and relate to the purposes of the exception.

When courts use the *Terry* reasonable suspicion standard to determine the reasonableness of warrantless "non-routine" border searches, the suspicion must arise at the border and relate to the purposes of the exception. Reasonable suspicion does "not justify unfettered crime-fighting searches or an unregulated assault on citizens' private information." *Cotterman*, 709 F.3d at 966.[18]

The suspicion must be of contemporaneous – not past – criminal activity specifically relating to the sovereign's interests in protecting its territorial integrity. *Montoya de Hernandez*, 473 U.S. at 541. Evidence of prior criminal activity does not supply reasonable suspicion. *United States v. Hassanshahi*, 75 F. Supp. 3d 101, 120 (D.D.C. 2014); *see also United States v. Walden*, 146 F.3d 489, 490 (7th Cir. 1998) ("reasonable suspicion of criminal activity cannot be based solely on a person's prior criminal record."). *See also United States v. Cortez*, 449 U.S. 411, 418 (1981) (border patrol agents had reasonable suspicion "that the particular individual being stopped *is engaged in* wrongdoing") (emphasis added).

[18] *Cotterman* can no longer support the conclusion that reasonable suspicion is sufficient for a forensic search of data because it was decided without the benefit of *Riley*. Nevertheless, as discussed below, were this Court to use the reasonable suspicion standard, the search here still does not comport with *Cotterman*.

Instead, "an investigatory stop must be justified by some objective manifestation that the person stopped *is, or is about to be*, engaged in criminal activity." *United States v. Cortez*, 449 U.S. 411, 417 (1981) (emphasis added). "The issue is whether a reasonably prudent man in the circumstances would be warranted in his belief that the suspect is breaking, or is about to break, the law." *United States v. Edmonds*, 240 F.3d 55, 59 (D.C. Cir. 2001).

The reasonable suspicion itself, in the present tense, must also be suspicion of threats at the border. An intrusive search based on reasonable suspicion "is justified at its inception if customs agents, considering all the facts and circumstances surrounding the traveler *and her trip*, reasonably suspect that the traveler *is smuggling contraband*." *Montoya de Hernandez*, 473 U.S. at 541 (emphasis added). Justifying an intrusive non-routine search requires "reasonable suspicion that the party to be searched is guilty of illegal concealment." *United States v. Ogberaha*, 771 F.2d 655, 657 (2d Cir. 1985).

For example, in *Cotterman*, the defendant was returning from what appeared to be a suspicious trip. The agents at the border knew that he was listed in the database because of an investigation into individuals involved in sex tourism, that he was a registered sex offender, that he was returning from a known sex tourism destination, had frequent travel to that destination, and had multiple cameras and

laptop. 709 F.3d at 968-69. In addition, an initial cursory review of the digital media revealed additional suspicious circumstances. *Id.* These facts, taken together, raised suspicion that the defendant, at that moment, was bringing contraband child pornography across the border in his digital devices.

Similarly, in *Hassanshahi*, while one factor was a prior criminal investigation into Iran trade embargo violations, the database hit revealed substantial information relating to the investigation and multiple prior suspicious trips. 75 F. Supp. 3d at 121-22. The travel itself was to Iran, and certain facts regarding the defendant's computer use while abroad, known to the agents at the border, demonstrated that the defendant was probably conducting business while in Iran. *Id.* at 122. In addition, the defendant carried multiple data storage devices, which indicated that the travel related to the same type of activity that he had been investigated for previously, i.e. conducting embargoed business activity with Iran. *Id.* at 123. These facts established reasonable suspicion that the defendant was actively engaged in criminal conduct as part of the instant travel, and that evidence of that illegal conduct was likely to be found in the data. *Id.*

Even in *Ickes*, where the issues were different, the facts apparent at the border established reasonable suspicion that the computer and disks contained contraband child pornography. The border patrol found marijuana and an open arrest warrant in

the car and saw photo albums with suspicious pictures of young children. The state of the vehicle was inconsistent with the defendant's explanation for his travel. And the officers conducted an initial brief search at the border in the defendant's presence. 393 F.3d at 503. Thus, the specific facts known to the border patrol when the defendant entered the United States established that the he was likely bringing contraband into the country in his stored data.

In addition, the suspicion must be that the specific search will be productive; if law enforcement agents do not have reason to believe that contraband or evidence of wrongdoing will be present in the item searched, they do not have reasonable suspicion. *Montoya de Hernandez* provides the perfect example: the x-ray would likely reveal whether the suspect was an alimentary canal smuggler. The Fourth Amendment never permits a general rummaging for evidence.

This connection between the suspicion and the object searched is particularly important when searching data. As discussed above, reasonable suspicion may be sufficient to support a brief, minimal intrusion into an individual's privacy rights. But when the law enforcement practice will intrude upon something as private as data on a smart phone, the government must have a particular basis for looking for the digital file. In *In re Grand Jury Subpoena Duces Tecum*, the Eleventh Circuit required a specific showing for the government to access data files: "Nothing in the

record before us reveals that the Government knows whether any files exist and are located on the hard drives." 670 F.3d 1335, 1346 (11th Cir. 2012). In order to grant the government access to the files, that court required "that the government show its knowledge *that the files exist.*" *Id.* at 1348 (emphasis supplied).[19]

Other data searches based on reasonable suspicion follow that practice. In both *Ickes* and *Cotterman*, the border patrol had specific reason to believe that reviewing the digital media was likely to uncover contraband. In *Hassanshahi*, because multiple circumstances led to suspicion that the defendant was returning from a business trip to Iran, his laptop and multiple digital devices were likely to contain evidence of prohibited transactions.

2. Warrantless searches based on reasonable suspicion must have a limited duration.

The unlimited duration of this search establishes that the search requires a warrant based upon probable cause, not just reasonable suspicion. Stops based on reasonable suspicion "cannot continue indefinitely." *United States v. Leo*, 792 F.3d 742, 750 (7th Cir. 2015). Reasonable suspicion can support certain stops and seizures because the stop or seizure is brief and highly circumscribed. The stop is reasonable

[19] Although this case address grand jury subpoenas and not warrantless searches, its reasoning is nevertheless instructive. The reasonable particularity requirement of a subpoena is analogous to what *Terry* requires.

precisely because it is brief. *United States v. Sharpe*, 470 U.S. 675, 68-87 (1985).

Because of the unlimited duration of forensic data searches, reasonable suspicion is insufficient to allow a warrantless search. The logical extension of holding otherwise would be to condone searching cell phone data during any *Terry* stop, which also requires only reasonable suspicion. But even before *Riley* foreclosed such an absurd result, there was no question that reasonable suspicion could not justify such a search. The Second Circuit had "little difficulty concluding" that an "extensive" search of a cell phone "went well beyond what was permissible under a *Terry* stop." *Carter v. City of Yonkers*, 345 Fed. Appx. 605, 606 (2d Cir. 2009). Similarly in the Fifth Circuit, searching a cell phone exceeds the "scope of a lawful protective search" under *Terry*. *United States v. Zavala*, 541 F.3d 562, 576 (5th Cir. 2008). Reasonable suspicion can support brief, limited intrusions, but not the exhaustive search for evidence that occurred here.

3. The facts here do not amount to reasonable suspicion.

In the 56-page memorandum opinion denying Mr. Saboonchi's motion to suppress, a single paragraph lists the facts that purported to establish reasonable suspicion. (JA 389.) The court stated that (1) Mr. Saboonchi's "name had come up" in two investigations into export violations; (2) information received in response to subpoenas showed that, in December 2010, Mr. Saboonchi had bought goods

representing that they would be used domestically, but shipped them to Dubai; (3) he had understated the value of the merchandise[20]; and (4) the recipient in Dubai "was linked to an industrial parts company in Iran." (JA 389. *See* JA 227-29.)

Only the first fact – that Mr. Saboonchi's "name had come up" – is relevant, because it is the only fact that Agent Baird knew when she entered Mr. Saboonchi's name into the database – when she decided to exploit the possibility of a border search. Every other fact listed came to the agent's attention later.

Moreover, this first fact is the only fact the CBP officer who searched Mr. Saboonchi and seized his electronic devices knew. He did not even know why Mr. Saboonchi's name appeared in the database (unlike *Cotterman*). And the mere presence of a name on the database, without more, does not establish reasonable suspicion that Mr. Saboonchi was engaged in criminal activity, was smuggling contraband, or was evading customs duties.

The rest of the facts establish, at most, a hunch that searching the phones and USB drive might uncover evidence of commercial transactions involving Iran from a year before. (JA 227-29.) That is insufficient to establish reasonable suspicion for a non-routine border search. Law enforcement was not confronted with an evolving

---

[20] The government does not dispute that, even if Mr. Saboonchi declared the full value, the amount fell below the threshold for excise taxes. (JA 231-32.)

situation, requiring immediate investigation, unlike *Ickes*, *Cotterman*, and *Montoya de Hernandez*, where failure to act immediately would have left the border vulnerable to contraband.

Nothing about Mr. Saboonchi's travel was suspicious. He carried no unusual quantity of digital devices. He answered questions in a way that allayed, rather than heightened suspicion. Nothing that the CBP officers observed was suspicious. The CBP officer had no need to use any particular training or experience to pick up on subtle cues.

None of the facts even hinted, let alone created any suspicion, that the two smart phones and USB drive themselves contained any contraband or evidence of wrongdoing. Here, no specific, articulable fact linked any suspicion to the cell phones or USB drive.

This search and the circumstances leading up to it were entirely unlike any of the border searches based on reasonable suspicion. Instead, it was almost indistinguishable from the search that occurred in *Kim*, which was unsupported by reasonable suspicion, and was unreasonable in light of *Riley*. In that case, the agents decided to conduct the search before the defendant traveled and had no reason to believe that the defendant was engaged in criminal activity at the border. At most, there was suspicion of a completed crime from some previous time. 2015 WL

2148070 at *9-10. The agent "was implementing a decision he had previously made elsewhere, and his collection of the laptop was not informed in any way by his observations on the scene, filtered through his training and experience or otherwise." *Id.* at *13. The court therefore suppressed the evidence.

This was not a scenario where the police believed a person might be armed, or needed to investigate an imminent danger. There was no split second decision necessary to allay or confirm suspicion. Instead, this search was a premeditated, discretionary choice, investigating past conduct, to develop evidence for a prosecution. Government agents took their time to execute a carefully orchestrated search.

The search here was a fishing expedition, nothing more. It violated *Riley*. It exceeded the scope of the border search doctrine. It lacked reasonable suspicion. Therefore, it was unreasonable under the Fourth Amendment. This Court should reverse the district court's decision and suppress the evidence.

II. The District Court improperly instructed the jury regarding the *mens rea* element of the offense by defining "willfully" as general knowledge of unlawfulness rather than an intentional violation of a known legal duty.

To convict Mr. Saboonchi, the government had to prove beyond a reasonable doubt that he knowingly and willfully exported embargoed items to Iran. 50 U.S.C. § 1705(c); 31 C.F.R. § 560.204. This element of willfulness is necessary because of

the complexity of the regulatory scheme at issue. Anything less could lead to convictions for innocent mistakes.

A. The statutory and regulatory scheme defining the crime of exporting to an embargoed country is a labyrinthine and sometimes contradictory web.

No single statute in the United States Code identifies the conduct that will subject an individual to either criminal or civil penalties for violating the Iran trade embargo. (JA 752.) Instead, a complex web of statutes, regulations, and executive orders combine to identify the proscribed conduct.[21]

Exporting similar items to Iran may be legal or illegal depending on whether the seller has a specific license allowing the particular transaction, has no license, or a general license allows similar transactions for certain purposes. Shipping goods to other countries may also violate the Iran embargo. Sending gifts to relatives is probably legal, but shipping the identical item to a commercial enterprise is probably illegal unless the exporter has a specific license. "General licenses" allow anyone to ship certain items to Iran at any time. (*See* JA 754.) Although a "general license" exists for shipments of academic and educational materials, some shipments that have

[21] The following statutes, regulations, and executive orders must be read in combination in order to identify what the ITSR prohibits: 50 U.S.C. §§ 1701, 1702 and 1705; 31 C.F.R. § 560.203; 31 C.F.R. § 560.204; Executive Order 12957; Executive Order 12959; and Executive Order 13059.

an academic purpose are embargoed regardless. (JA 755.) And shipments of some items are simply exempt from the embargo. (JA 763.)

Not every approved or prohibited transaction is readily apparent from the regulations. (JA 753.) The Office of Foreign Asset Control (OFAC), which administers these regulations and issues export licenses, sometimes updates its web site with information about changes to what is embargoed and what is permissible, although the changes do not yet appear in the regulations themselves. (JA 753.)

OFAC has an entire staff dedicated to clarifying confusion on the part of would-be exporters. Sometimes, it issues "interpretive guidance" on its web site when OFAC perceives a need to clarify the regulations. (JA 755-56.) It also staffs a hotline to answer questions. Many of these questions come from attorneys who are advising corporate clients.[22] (JA 756.) OFAC also accepts written questions from confused exporters, but it does not respond to all requests for guidance. (JA 756.) A section of OFAC's web site answers "Frequently Asked Questions" explaining

[22] These sanctions are sufficiently complex that most white-shoe law firms in Washington, DC, and elsewhere have entire practice groups specializing in sanctions compliance and enforcement. A few of the many examples include: Shearman & Sterling (http://www.shearman.com/en/services/key-issues/iran-sanctions); Davis Polk (http://www.davispolk.com/practices/litigation/economic-sanctions-national-security); Sidley Austin (http://www.sidley.com/en/services/sanctions) Vinson & Elkins (http://velaw.com/What-We-Do/Export-Controls---Economic-Sanctions/); Reed Smith (http://www.reedsmith.com/sanctions/).

exporters' legal obligations. It lists *396* FAQ's. (JA 759.)

OFAC offers compliance guidance in other languages, but Farsi is not one of them. Farsi, however, is the native language of Iran and is Mr. Saboonchi's primary language. (JA 760.)

Confusion surrounding this mare's nest of regulations, guidance, updates, and executive orders extends beyond just potential exporters to the special agents charged with investigating criminal violations of the ITSR. Special Agent Baird had never been trained on what the ITSR covered and had never actually read the regulations. (JA 707, 708.) Instead, she only saw an OFAC summary. (JA 708.)

When Agent Baird discussed Mr. Saboonchi's connections to Iran with him, both were confused about what was permitted. She was unsure whether an internship that Mr. Saboonchi held while he was a student in Iran qualified as a "service" needing a specific license. (JA 715-16.) In addition, Mr. Saboonchi told her that he thought certain activities were subject to the embargo – for example, flying on Iran Air – that she was either unsure of, or that she believed were permissible. (JA 730-31.) She suggested that he look at the OFAC web site (and its 396 FAQ's) to figure out what he could do, but gave him no written information, summaries, or even the internet address. (JA 719.)

B. To save this virtually impenetrable web of regulations from unconstitutional vagueness, the government must prove a specific intent *mens rea* of willfulness to secure a conviction.

The IEEPA and ITSR explicitly include a specific intent *mens rea*. Violations of the ITSR only constitute a crime, rather than a civil infraction, if committed knowingly and wilfully. 50 U.S.C. § 560.204.

This wilfulness element is essential to due process because crimes based on complex regulatory schemes, like the IEEPA and ITSR, risk failing to give fair notice of what is prohibited. But with an element of willfulness, the "scienter requirement may mitigate a law's vagueness," ensuring that nobody is convicted unless they are aware of what the law prohibits. *United States v. Amirnazmi*, 645 F.3d 564, 589 (3d Cir. 2011) (internal quotation omitted). The element of willful intent makes the conduct inconsistent with "surprised innocence." *Id.*

When charged with violating the ITSR, "ignorance of the law *is* a defense." *Amirnazmi*, 645 F.3d at 589. A defendant is only guilty of a criminal violation if he "actually knew of the prohibition against dealing with [the country] . . . and deliberately violated it." *United States v. Macko*, 994 F.2d 1526, 1533 (11th Cir. 1993) (addressing the Cuban embargo). The government must prove that the defendant knew of the licensing requirements set out in the regulations. *See United States v. Elashyi*, 554 F.3d 480, 495 (5th Cir. 2008). Since the "activities denoted

unlawful are spelled out in criminal regulations and include items not known generally to be controlled by the government, the regulatory provisions must be actually known and intentionally violated for a crime to be committed." *United States v. Frade*, 709 F.2d 1387, 1392 (11th Cir. 1983) (internal quotations omitted). *But see United States v. Brodie*, 403 F.3d 123, 147 (3d Cir. 2005) (holding that a general knowledge of the embargo is sufficient, and failing to "brush up on the law" is not a defense against charges of violating the Cuban embargo).

This definition of specific intent is consistent with Supreme Court interpretations of "willfulness" when addressing complex regulatory crimes that prohibit conduct that is not obviously unlawful. For example, since "the proliferation of statutes and regulations has sometimes made it difficult for the average citizen to know and comprehend the extent of the duties and obligations imposed by the tax laws," specific intent is required. *Cheek v. United States*, 498 U.S. 192, 199-200 (1991). The complexity of the law requires a softening of "the impact of the common law presumption" that ignorance of the law is no defense. *Id.* at 200.

In complex regulatory arenas, willfulness means that a defendant voluntarily and intentionally violated a "known legal duty." *Cheek*, 498 U.S. at 200. *See also United States v. Pomponio*, 429 U.S. 10, 12 (1976). Said another way, when crimes are defined by complex regulations, the government must "prove that the law imposed

a duty on the defendant, that the defendant knew of this duty, and that he voluntarily and intentionally violated that duty." *Cheek,* 498 U.S. at 201.

The labyrinthine regulations, executive orders, and statutes that comprise the Iranian trade embargo embody just such a scheme where the *Cheek* definition of wilfulness is necessary. Since exporting similar items may be permissible, falling under a "general license" if used for the purpose of academia, or could require applying for a special license, and since shipping some items does not require any license at all, "average citizens" would have exceptional difficulty in understanding what the law prohibits and permits. *Compare Cheek*, 498 U.S. at 199. The criminal conduct is not obviously wrong; it is the classic *malum prohibitum* offense.

The government's sentencing evidence highlighted this conundrum. Since the goods Mr. Saboonchi shipped were not inherently dangerous, the government tried to paint Mr. Saboonchi's conduct in the most sinister light, trying to make his conduct appear obviously wrong. In actuality, the evidence bolstered the fact that the embargo prohibits shipments of "benign" items, making it difficult for an average person to know what is lawful and what is illegal.

The government introduced expert testimony of an analyst at the Lawrence Livermore National Laboratory, a government facility for researching nuclear weapons, to opine about "possible nefarious uses" for the goods Mr. Saboonchi

shipped to Dubai and China. (JA 2802.) The specific direction that the FBI gave to the analyst was to "get [an] unclass[ified] letter providing some detail on the nuclear applications of subject's [Mr. Saboonchi's] activities." (JA 2824.) The scientist, however, refused to give the government the opinion that it sought.

He stated that the goods could equally "be used in a benign fashion for commercial activities" although some items could have uses in nuclear technology as well. (JA 2807.) He reached that conclusion because some items were non-corrosive – made from stainless steel. FBI supervisors requested revisions to his opinion letter to include "more language linking Mr. Saboonchi's conduct to Iran's nuclear program." (JA 2835.) The expert responded that he could not provide that opinion. (*Id.*) In fact, his initial draft described the goods as "mostly generic," but at the FBI's direction, that phrase was deleted from the final opinion letter. (JA 2837-38.)

The goods had "many applications." (JA 2817.) Indeed, some of the items are available at a Home Depot, local hardware stores, or vacuum cleaner repair stores. (JA 2813. 2832.) In addition to having applications in chemical, oil and gas, and power generation, the goods had applications in "food, beverage and dairy, medical and dental" spheres. (JA 2833.) Even the items that were safe for use in the nuclear industry were not the sort that enhanced, transported, or stored nuclear materials.

Instead, the spare parts were the type that are designed for sampling particles, and could as easily be used for safety in medical practices. (JA 2839.)

Thus the "unlawful" character of sending these items is not readily apparent. When updates to the regulations may only be published on the internet and not in the actual regulations, special agents are unsure of what the embargo covers, and one must read 396 FAQ's when seeking guidance, the government must prove that the defendant knew what his legal obligations were, and voluntarily violated those known legal duties. Otherwise, a person cannot be said to have committed this regulatory crime.

C. The jury instructions here incorrectly defined wilfulness.

The district court incorrectly instructed the jury regarding willfulness because it did not require the government to prove that Mr. Saboonchi knew what the IEEPA and ITSR prohibited, yet chose to violate the regulations anyway. Instead, the instruction allowed the jury to convict Mr. Saboonchi if he knew, in general terms, that his conduct was "unlawful." The instruction stated, "While the government must show that the defendant knew that his conduct was unlawful, it is not necessary for the government to prove that the defendant had read or *was aware of* the contents of the IEEPA or the ITSR." (JA 2631) (emphasis added).

This instruction eliminated the essential characteristic of wilfulness: that the

defendant knowingly and voluntarily violated a known legal duty. Unless the government proved that Mr. Saboonchi knew what the contents of the IEEPA and ITSR were, it could not establish that he knew of the duty that the law imposed on him but nevertheless specifically chose to violate it. *See Cheek*, 498 U.S. at 201. This instruction allowed the jury to convict if it decided that Mr. Saboonchi acted out of ignorance or negligence. It allowed a conviction based upon a general intent to commit the conduct, thinking only that the exports might not be allowed, rather than the specific intent that the IEEPA and ITSR explicitly require.

The district court's legal error in incorrectly defining the intent element constituted an abuse of discretion. *See Gunnells v. Healthplan Servs. Inc.*, 348 F.3d 417, 446 (4th Cir. 2003). *Staples v. United States*, 511 U.S. 600, 605 (1994) (explaining that determining the mental state is a question of statutory interpretation). "An abuse of discretion occurs where the district court applies the wrong law." *United States v. Brown*, 415 F.3d 1257, 1266 (11th Cir. 2005).

The district court improperly relied on *Bryan v. United States*, 524 U.S. 184 (1998). In that case, the defendant was charged with conspiring to sell firearms without a license. The defendant requested an instruction that required proof that he had "actual knowledge of the federal firearms licensing laws, and acted in knowing violation of them." *Id.* at 190 n.10. Instead, the trial court gave an instruction similar

to what the court gave here. The Court held that to prove a willful violation of the statute, "the jury must find that the defendant acted with an evil-meaning mind, that is to say, that he acted with knowledge that his conduct was unlawful." *Id.* at 194.

Bryan, however, does not control the result here. The case itself discusses the fact that criminal violations of complex regulatory schemes require a heightened scienter requirement, more than knowledge that conduct is unlawful. 524 U.S. at 194. In those complex regulatory arenas, "willfully" means that the defendant knows of the actual provision in the statute or regulation that prohibits the defendant's conduct. *Id.* These complex regulatory crimes require specific knowledge of the law because that type of law "sometimes criminalize[s] conduct that would not strike the ordinary citizen as immoral or likely unlawful. Thus, [the] sets of laws may lead to the unfair result of criminally prosecuting individuals who subjectively and honestly believe they have not acted criminally." *Id.* at 195 n.22 (quoting *United States v. Aversa*, 984 F.2d 493, 502 (1st Cir. 1993)).

The statutory scheme in *Bryan* does not share a comparable level of complexity with the ITSR. *See* 524 U.S. at 188 n.4, 189 n.5. Trafficking in firearms is the kind of conduct that ordinary citizens are likely to understand is unlawful. It involves inherently dangerous items and the average citizen knows that criminal laws address issues surrounding firearms. The same cannot be said here. Even if people have a

general understanding that an embargo against Iran exists, the testimony of the OFAC representative, and the lack of understanding of the regulations evinced in the HSI special agent's testimony make clear that any general understanding cannot approach differentiating between what is sometimes lawful and sometimes unlawful.

The district court also incorrectly relied on *United States v. Bishop*, where this Court determined the mental state for violating the Arms Export Control Act. 740 F.3d 927 (4th Cir. 2014). The defendant argued that the statute required proof that he knew why the conduct was criminal. *Id*. at 932. This Court disagreed, and found that "nothing in the language or purpose of the statute suggested that Congress wished to jettison altogether the bedrock presumption that each of us knows the standards applicable to our personal conduct." *Id*. at 934. Violations of the Arms Export Control Act require "only a general knowledge of illegality." *Id.* at 935.

The statute at issue in *Bishop*, however, is not analogous to the ITSR. This Court explained that the Arms Export Control Act "does not include such highly technical requirements as might inadvertently criminalize good faith attempts at compliance." *Id.* at 933. Unlike highly technical areas of law, "the export of 9mm and AK-47 ammunition to Jordan would quickly strike someone of ordinary intelligence as potentially unlawful." *Id.* Although it is a regulatory offense, it lacks the purely *malum prohibitum* nature of the ITSR. Instead, shipping AK-47

ammunition overseas simply sounds illegal, unlike shipping products that appear to have wholesome uses, like improving medical safety or dairy production.

Furthermore, *Bishop* acknowledged the different versions of willfulness, and acknowledged that the regulatory scheme it was addressing was relatively straightforward. *Bishop* therefore does not provide this Court's final and only definition of "willfulness." While this Court has not addressed the intent element of the ITSR, the reasoning in *Bryan* and *Bishop* actually supports the conclusion that the *Cheek* standard is the correct standard here.

Finally, the instruction here lightened the government's burden, contrary to what other courts have used for instructing on the intent element of violating the Iran trade embargo. Prosecutions for this particular offense are relatively rare, with cases resolved by jury trial even rarer,[23] meaning that actual jury instructions are difficult to come by, even in reported cases. Several examples, however, do exist. In *United States v. Mousavi*, the district court instructed the jury consistently with *Cheek*: "Fourth, the defendant acted wilfully, that is, voluntarily and intentionally in violation of a *known legal duty*."[24] In *United States v. Alavi*, the jury instruction on specific

---

[23] *See* Mr. Saboonchi's sentencing memo, District Court Docket Entry 248, at pp. 12-17, compiling a list of prosecutions.

[24] Docket Entry 130 at p. 24, Case No. 2:07-cr-00513-PA (C.D. Cal.) (April 21, 2008) (emphasis added). The opinion after appeal in this case is reported t 604 F.3d

intent defined willfully: "that is, voluntarily and intentionally in violation of a *known legal duty not to export the good*."[25] In *United States v. Modanlo*, from the same district where this case arose, the instruction stated, "To find the defendant . . . guilty [of] . . . conspiring to willfully violate a regulation issued pursuant to IEEPA, or . . . willfully violating or attempting to violate such a regulation, the government must prove beyond a reasonable doubt that *he knew his actions violated the Iranian Transaction Regulations*."[26] Here, in contrast, a general sense of unlawfulness sufficed. The other cases all require a specific understanding of the legal obligations that the regulations impose.

The jury instruction here reduced the government's burden of proving the intent element. The actual *mens rea* element requires proof that the defendant knew what his legal obligations were under the ITSR, but he intentionally violated that known legal duty. Yet the district court instructed the jury that it could convict Mr. Saboonchi if he had a general sense that what he was doing was unlawful. Mr.

1084 (9th Cir. 2010).

[25] Government Proposed Jury Instruction, Docket Entry 313 at p. 2, Case No. 2:07-cr-429-NVW (D. Ariz.) May 20, 2008.

[26] Docket Entry 453 at p. 54, Case No. 8:10-cr-295-PJM (Sept. 26, 2013) (emphasis added). An appeal in this case is pending in this Court. Fourth Cir. Case No. 14-4044.

Saboonchi was thereby hamstrung in arguing to the jury that he did not know or understand exactly what the embargo prohibited. The court told the jury that it did not matter if Mr. Saboonchi knew what the ITSR prohibited. This Court should therefore remand for a new trial.

CONCLUSION

The search of Mr. Saboonchi's iPhone and USB drive was unreasonable under the Fourth Amendment. In addition, the court improperly instructed the jury regarding the specific intent element of the offense, prejudicing Mr. Saboonchi's ability to argue that he lacked the necessary *mens rea*. This Court should therefore enter an order suppressing the evidence and granting him a new trial.

JAMES WYDA
Federal Public Defender
District of Maryland

/s/
MEGHAN SKELTON
Appellate Attorney
6411 Ivy Lane, Suite 710
Greenbelt, MD 20770
(301) 344-0600
Counsel for Appellant

REQUEST FOR ORAL ARGUMENT

This case presents a question relating to a substantial violation of the defendant's Fourth Amendment and privacy rights. He therefore requests oral argument.

CERTIFICATE OF COMPLIANCE

1. This Brief of Appellant has been prepared using WordPerfect X4 software, Times New Roman font, 14 point proportional type size.

2. Exclusive of the table of contents, table of authorities, statement with respect to oral argument, and certificate of service, this brief contains 13,462 words.

I understand that a material misrepresentation can result in this Court's striking the brief and imposing sanctions. If the Court so requests, I will provide a copy of the word or line print-out.

09/03/2015
Date

/s/
Meghan Skelton
Appellate Attorney

CERTIFICATE OF SERVICE

This is to certify that the foregoing Brief of Appellant was filed electronically via CM/ECF, and a hard copy of the Brief of Appellant and Joint Appendix were sent via inter-office mail to:

Christine Manuelian
Assistant U.S. Attorney
Office of the U.S. Attorney
36 South Charles Street
Fourth Floor
Baltimore, MD 21201

on this 3rd day of September, 2015.

/s/
Meghan Skelton
Appellate Attorney