990 F.Supp.2d 536
United States District Court,
D. Maryland,
Southern Division.

UNITED STATES of America
v.
Ali SABOONCHI, et al.

Criminal Case No. PWG–13–100.
|
Signed April 7, 2014.

Synopsis

Background: Defendant, indicted for multiple counts of unlawful export to an embargoed country and one count of conspiracy to export to an embargoed country, in violation of the International Emergency Economic Powers Act (IEEPA) and the Iranian Transactions and Sanctions Regulations (ITSR), moved to suppress evidence obtained during warrantless forensic searches of his smartphones and flash drive.

Holdings: The District Court, Paul W. Grimm, J., held that:

[1] reasonable suspicion was required for performance of forensic searches of digital devices taken from defendant at border, and

[2] reasonable suspicion existed to support such search.

Motion denied.

West Headnotes (19)

[1] Customs Duties
Searches and Seizures

Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border, and thus searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into the country, are reasonable, within meaning of the Fourth Amendment, simply by virtue of the fact that they occur at the border. U.S.C.A. Const.Amend. 4.

Cases that cite this headnote

[2] Customs Duties
Grounds or cause for stop, search, or seizure

Routine searches of the persons and effects of entrants at a border are not subject to any requirement of reasonable suspicion, probable cause, or warrant. U.S.C.A. Const.Amend. 4.

Cases that cite this headnote

[3] Customs Duties
Searches and Seizures

Even at the border, Fourth Amendment continues to protect against unreasonable searches and seizures. U.S.C.A. Const.Amend. 4.

Cases that cite this headnote

[4] Customs Duties
Searches and Seizures

At the border, routine searches become reasonable within meaning of the Fourth Amendment because the interest of the Government is far stronger and the reasonable expectation of privacy of an individual seeking entry is considerably weaker. U.S.C.A. Const.Amend. 4.

Cases that cite this headnote

[5] Customs Duties
Grounds or cause for stop, search, or seizure

When a border search stretches beyond the routine, it must rest on reasonable, particularized suspicion, which is significantly less demanding than the showing of probable

cause required to secure a warrant for a domestic search. U.S.C.A. Const.Amend. 4.

Cases that cite this headnote

[6] **Searches and Seizures**
Scope, Conduct, and Duration of Warrantless Search

Under the Fourth Amendment, mere fact that a search includes computer files does not transform it from routine to nonroutine. U.S.C.A. Const.Amend. 4.

Cases that cite this headnote

[7] **Customs Duties**
Time and distance factors;checkpoints

Under the Fourth Amendment, a border search need not take place at the border. U.S.C.A. Const.Amend. 4.

Cases that cite this headnote

[8] **Customs Duties**
Time and distance factors;checkpoints

Customs Duties
Airports and airplanes

Under the Fourth Amendment, border searches may in certain circumstances take place not only at the border itself, but at its functional equivalents as well; the functional equivalent of a border may include an established station near the border, at a point marking the confluence of two or more roads that extend from the border, or the search of passengers and cargo arriving at an airport within the United States after a nonstop flight from abroad. U.S.C.A. Const.Amend. 4.

Cases that cite this headnote

[9] **Customs Duties**
Time and distance factors;checkpoints

Extended border search doctrine has been applied to entry border searches conducted some time after the border was crossed.

1 Cases that cite this headnote

[10] **Customs Duties**
Time and distance factors;checkpoints

Unlike searches that actually occur at a border or the functional equivalent thereof, an extended border search requires reasonable suspicion with respect to the criminal nature of the person or thing searched as well as reasonable suspicion that the subject of the search has crossed a border within a reasonably recent time. U.S.C.A. Const.Amend. 4.

2 Cases that cite this headnote

[11] **Customs Duties**
Time and distance factors;checkpoints

Government agents' search of defendant's electronic devices was not an extended border search within meaning of the Fourth Amendment; the devices did not enter the country with defendant, but were returned to him at a later date. U.S.C.A. Const.Amend. 4.

Cases that cite this headnote

[12] **Customs Duties**
Time and distance factors;checkpoints

A border search of a computer is not transformed into an extended border search under the Fourth Amendment simply because the device is transported and examined beyond the border. U.S.C.A. Const.Amend. 4.

3 Cases that cite this headnote

[13] **Customs Duties**
Grounds or cause for stop, search, or seizure

A forensic border search of a computer or electronic device should be considered a nonroutine search for which reasonable suspicion is required under the Fourth Amendment. U.S.C.A. Const.Amend. 4.

4 Cases that cite this headnote

[14] Customs Duties

Personal, skin, or strip searches;pat-down

Even the border search power cannot justify a strip search without any particularized suspicion. U.S.C.A. Const.Amend. 4.

Cases that cite this headnote

[15] Customs Duties

Grounds or cause for stop, search, or seizure

A border search that goes beyond the routine is justified merely by reasonable suspicion, a lesser standard than required for analogous non-border searches. U.S.C.A. Const.Amend. 4.

Cases that cite this headnote

[16] Searches and Seizures

Scope, Conduct, and Duration of Warrantless Search

Even if a search is not destructive or damaging, if it is sufficiently invasive or intrusive, or butts up against other Fourth Amendment values, it may be nonroutine. U.S.C.A. Const.Amend. 4.

Cases that cite this headnote

[17] Customs Duties

Scope and Nature;Successive or Secondary Searches

Under the Fourth Amendment, a routine border search may include a conventional inspection of electronic media and a review of the files on them just as it may include physical papers. U.S.C.A. Const.Amend. 4.

2 Cases that cite this headnote

[18] Customs Duties

Time and distance factors;checkpoints

Reasonable suspicion was required for forensic search of imaged hard drives of digital devices taken from defendant at the border and subjected to forensic examination at later time; search would result in exposure of intimate details and abrogate defendant's reasonable expectations of privacy in his most personal and confidential affairs. U.S.C.A. Const.Amend. 4.

2 Cases that cite this headnote

[19] Customs Duties

Grounds or cause for stop, search, or seizure

Reasonable suspicion supported forensic search of smartphone and flash drive taken from defendant as he crossed border; defendant's name had come up in connection with two different investigations of export violations, information received in response to previously-issued subpoenas showed that he had purchased two cyclone separators after representing that they would be used domestically, and then shipped them overseas, understating their value in a manner consistent with an attempt to avoid scrutiny, and investigation had determined that the recipient of the separators was linked to a company in Iran. U.S.C.A. Const.Amend. 4.

Cases that cite this headnote

Attorneys and Law Firms

***538** Christine Manuelian, Rod J. Rosenstein, Office of the United States Attorney, Baltimore, MD, for United States of America.

***539** Elizabeth Genevieve Oyer, Office of the Federal Public Defender, Baltimore, MD, for Ali Saboonchi, et al.

MEMORANDUM OPINION

PAUL W. GRIMM, District Judge.

Defendant Ali Saboonchi is alleged to have violated U.S. export restrictions on trade with the Islamic Republic of Iran. On July 18, 2013, Saboonchi moved to suppress the fruits of warrantless forensic searches of his smartphones and flash drive performed under the authority of the border search doctrine after they were seized at the U.S. —Canadian border. At a hearing on September 23, 2013, I issued an oral opinion denying the motion but stated that, in light of the difficult issues raised by a forensic search of digital devices seized at the border, I would be issuing a written opinion further explaining my reasoning. Supplemental briefing was requested and permitted. I now hold that, under the facts presented by this case, a forensic computer search cannot be performed under the border search doctrine in the absence of reasonable suspicion. Because the officials here reasonably suspected that Saboonchi was violating export restrictions, Defendant's Motion to Suppress is denied.

I. BACKGROUND

Defendant Ali Saboonchi is a dual citizen of the United States and the Islamic Republic of Iran. Gov't Opp'n 3, ECF No. 65. On March 4, 2013, Saboonchi was indicted by a grand jury on four counts of unlawful export to an embargoed country and one count of conspiracy to export to an embargoed country, in violation of the International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C. §§ 1702 & 1705, and the Iranian Transactions and Sanctions Regulations ("ITSR"), 31 C.F.R. § 560.203–204. *See* Indictment, ECF No. 1. On August 22, 2013, the grand jury returned a superseding indictment that added more alleged co-conspirators, an additional count, and additional acts in furtherance of the alleged conspiracy, and revised the alleged start of the conspiracy from November 2009 to September 2009. Superseding Indictment, ECF No. 66. [1]

[1] On December 12, 2013, subsequent to the hearing on this motion, a second superseding indictment was returned that added an additional count against Saboonchi. *See* Second Superseding Indictment, ECF No. 95.

On July 18, 2013, Saboonchi filed several motions including a Motion to Suppress Evidence, ECF No. 58.

Most of the basic facts are undisputed. Saboonchi and his wife were stopped by United States Customs and Border Protection ("CBP") agents on March 31, 2012 at the Rainbow Bridge outside of Buffalo, New York when returning from a daytrip to the Canadian side of Niagara Falls. Def.'s Mot. 2. Saboonchi and his wife were questioned separately, and Saboonchi was questioned in a locked room where he was "required to remain in the room and directed to answer questions by a federal agent." *Id.* "Without Defendant's knowledge and consent, all electronics were seized with intent to search." *Id.* at 3. Eventually, Saboonchi and his wife were allowed to reenter the United States, but an Apple iPhone, a Sony Xperia phone, and a Kingston DT101 G2 USB flash drive (the "Devices") were seized; Saboonchi claims that "no clear justification was given for" keeping the Devices. *Id.* Saboonchi was given a "Detention Notice and Custody Receipt for Detained Property," CBP Form 6051D, listing the devices. CBP Form 6051D, Def's Mot. Ex. B, ECF No. 58–2.

***540** On April 4, 2012, a Homeland Security Investigations ("HSI") special agent imaged each of the Devices, *see* ICE Report of Investigation Continuation (the "ICE Reports"), Def.'s Mot. Ex. A, ECF No. 58–1. [2] Thereafter, the image of each device was forensically searched using specialized software. *Id.*

[2] Imaging a hard drive is the first step of a forensic search and involves making a copy of a storage device that is known as an "image," "bitstream" copy, or "forensic" copy. *See* Orin S. Kerr, *Searches and Seizures in a Digital World,* 119 Harv. L.Rev. 531, 540–41 (2005). "A Bit Stream Backup is an exact copy of a hard drive, preserving all latent data in addition to the files and directory structures." The Sedona Conference Glossary: E–Discovery & Digital Information Management 6 (3d ed.2010).

On April 13, 2012, Saboonchi met with two HSI agents in Baltimore who returned the Devices to him. Def.'s Mot. 6; Gov't Opp'n 25. At that time, a conversation occurred that Saboonchi characterized as an "interrogat[ion]," Def.'s Mot. 6, and that, at the very least, confirmed that Saboonchi owned two of the Devices and included questioning about an internship Saboonchi once had with an Iranian company and his knowledge of restrictions on doing business with Iran, Gov't Opp'n 25.

Saboonchi moved to suppress any evidence obtained from the Devices, any statements that he made to CBP on March 31, 2012, and any statements that he made to HSI on April 13, 2012. *See* Def.'s Mot. Saboonchi's

motion relied on his argument that the warrantless search of the Devices at the border—and their later forensic search—violated the Fourth Amendment's prohibition of unreasonable searches and seizures, *id.* at 7–8, that any statements made on March 31 were obtained in violation of the Fifth Amendment's Self–Incrimination Clause, *id.* at 6–7, and that any statements made on April 13 resulted from the improper search of Saboonchi's Devices, *id.,* and therefore are the "fruit of the poisonous tree," *Nardone v. United States,* 308 U.S. 338, 341, 60 S.Ct. 266, 84 L.Ed. 307 (1939). The Government responded, taking the position that the search of the Devices was a routine border search that required neither a warrant nor particularized suspicion and that Saboonchi's statements did not result from custodial interrogation. Gov't Opp'n 28–29. Shortly before the hearing on the motion to suppress, I sent a letter to the parties seeking additional briefing as to certain matters, Letter to Counsel (Sept. 13, 2013), ECF No. 73, and the parties responded shortly thereafter, *see* Gov't Supp. Mots. Resp., ECF No. 75; Def.'s Supp. Briefing Submission, ECF No. 76.

A hearing was held before me on September 23, 2013, at which the Government presented testimony from two witnesses: CBP Officer Kenneth Burkhardt, *see* Hr'g Tr., Testimony of Kenneth Burkhardt ("Burkhardt Tr."), ECF No. 85, and HSI Special Agent Kelly Baird, *see* Hr'g Tr., Testimony of Kelly Baird ("Baird Tr."), ECF No. 84.

A. Testimony of Kenneth Burkhardt

Officer Burkhardt was one of the officers who performed a secondary screening on Saboonchi when he re-entered the United States via the Rainbow Bridge in Niagara Falls, New York on March 31, 2013, Burkhardt Tr. 6:4–9, and his testimony primarily relied on his recollection as refreshed by his report of the events of March 31, 2012, as well as his knowledge of standard practices at the Rainbow Bridge facility. According to Burkhardt, people traveling by car go through primary screening in one of about seventeen lanes. *Id.* at 6:17–21. Although Burkhardt lacked firsthand knowledge of Saboonchi's primary inspection, it was his understanding that Saboonchi arrived at ***541** the Rainbow Bridge facility at 9:47 p.m., *id.* at 22:11, and was referred to secondary inspection because his name had produced a "hit" in the TECS database during primary screening, *id.* at 38:11–17. [3]

[3] TECS (not an acronym) is the updated and modified version of the former Treasury Enforcement Communications System. TECS is owned and managed by the U.S. Department of Homeland Security's (DHS) component U.S. Customs and Border Protection (CBP). TECS is the principal system used by officers at the border to assist with screening and determinations regarding admissibility of arriving persons.

U.S. Dep't of Homeland Sec., *Privacy Impact Assessment Update for the TECS System: CBP Primary and Secondary Processing (TECS) National SAR Initiative* 2 (Aug. 5, 2011), *available at* https://www.dhs. gov/xlibrary/assets/privacy/privacy-pia-cbp-tecs-sar-update.pdf.

In general, once a car is diverted to secondary inspection, it is approached by one or more officers, with weapons holstered, to escort the car to secondary inspection. *Id.* at 7:13–8:15. When the car reaches the main CBP building, a "stop stick" tire deflation device is placed between the front and back tires of the car to prevent flight. *Id.* at 17:20–23. The passengers are escorted inside and a secondary inspection typically is conducted in a room off of the building's lobby called the "medium secondary." *Id.* at 9:11–16. The medium secondary is reached through a locked door, which is operated remotely to buzz people in or out. *Id.* at 15:17–16:5. The room contains several chairs and a metal table, *id.* at 15:7–16:5; Hr'g Ex. 1F–1H, and has windows that are tinted on their bottom portion. *See* Hr'g Ex. 1F–1H. Saboonchi and his wife were taken into the secondary inspection area and Officer Burkhardt took their passports and Saboonchi's wife's visa. Burkhardt Tr. 18:8–19:24.

Burkhardt ran his own query of TECS and discovered two flags on Saboonchi, one out of Washington, D.C. and one out of Baltimore. *Id.* at 20:5–7. Because of those flags, at 9:52 p.m., Burkhardt contacted HSI Special Agent Kelly Baird about Saboonchi; Baird told him to detain Saboonchi's Devices. *Id.* at 20:8–23; 22:11–12.

At 10:00 p.m., Burkhardt interviewed Saboonchi and his wife. *Id.* at 22:15. The interview consisted of routine questions regarding their citizenship, their reason for traveling to Canada, and other information relevant to their readmission to the United States. *Id.* at 23:21–24:10. The interview did not last more than thirty minutes, and may have been as short as ten to fifteen minutes. *Id.* at 29:3–20. Burkhardt did not give *Miranda* warnings to Saboonchi or his wife, *id.* at 31:7–9, and testified that they

> are allowed to refuse to answer questions, but until we determine their admissibility, I mean, a thorough search of the car, a thorough search of them, I mean, we are going to, so to speak, get to the bottom of what we want to—I mean, 99.9 percent of people answer questions.

Id. at 68:2–6. Although Burkhardt did not recall the details of questioning Saboonchi and his wife, he stated that his standard practice would be to separate a car's passengers and question them separately. *Id.* at 33:11–14. At this time they also would have been asked to empty their pockets, known as a "pocket dump," *id.* at 21:14–18, 65:16–21, but they probably were not subjected to a pat-down or other more invasive search of their persons, *id.* at 30:16–22. At approximately 10:30 p.m., a "seven-point exam," which is a detailed examination of Saboonchi's car, was performed. *Id.* at 22:18–23:2. Saboonchi and his wife were not free to leave during this process. *Id.* at 46:17–47:14.

***542** The HSI duty agent at the Rainbow Bridge, Cornelius O'Rourke, was contacted at 10:55 p.m. and responded at 11:20 p.m. *Id.* at 23:9–12. At 11:55 p.m., HSI Special Agent Kelly Baird requested that all of the Saboonchis' information be turned over to the local Joint Terrorism Task Force ("JTTF") agent, Jeff Alrich. *Id.* at 23:12–15. The local chief was informed of all that had transpired at 12:15 a.m. on April 1, 2013, and Saboonchi and his wife were released at 12:25 a.m. on April 1. *Id.* at 23:16–17. From when they were stopped until they were cleared to enter the United States, over two and one-half hours had elapsed.

Although Saboonchi and his wife were allowed to re-enter the country, the Devices were not returned to them at that time and Saboonchi was given a CBP 6051D receipt for the detention of the Devices. CBP Form 6051D. Burkhardt said that it was not normal practice to look at the contents of electronic media found on a person during inspection, *id.* at 41:4–43:25, and neither he nor any other CBP officer attempted even a cursory inspection of the contents of the Devices at the Rainbow Bridge, *id.* at 59:13–60:1. "Duty Agent O'Rourke departed the station with the two cell phones and the thumb drive." *Id.* at 24:19–20.

In Burkhardt's view, what happened at the screening was "[a]bsolutely routine." *Id.* at 28:23.

B. Testimony of Kelly Baird

Special Agent Kelly Baird testified on three main issues: the factual basis underlying the flags on Saboonchi in the TECS database, the forensic searches of the Devices, and her April 13, 2012 meeting with Saboonchi to return the Devices.

Baird testified that Saboonchi first came to the attention of federal authorities in the Fall of 2010, when "the FBI received information that there had been an inquiry to a company in Vermont regarding specialized technology that has applications with industrial medical or military applications" by "a person named Ali," whose telephone number eventually led to Saboonchi. Baird Tr. 10:21–11:2. Around December 2011, another HSI agent contacted Baird to inform her that Saboonchi's name had come up again in the context of another investigation into export violations. *Id.* at 11:19–23. This led HSI to issue a number of subpoenas seeking credit card and shipping records that were returned in early March 2012. *Id.* at 11:24–12:2. [4]

[4] Saboonchi does not appear to have challenged the investigation up to this point; nor is it clear that he would have standing to challenge subpoenas issued to unrelated third parties in any event. *See United States v. Payner,* 447 U.S. 727, 732, 100 S.Ct. 2439, 65 L.Ed.2d 468 (1980) ("[A] court may not exclude evidence under the Fourth Amendment unless it finds that an unlawful search or seizure violated *the defendant's own* constitutional rights." (emphasis added) (citation omitted)).

In response to HSI's subpoenas, Baird received a Federal Express ("FedEx") airbill that showed that Ali Saboonchi, through a business called Ace Electric, had shipped a cyclone separator to an Arash Rashti at a company called General DSAZ in the United Arab Emirates. *Id.* at 12:2–7, 29:1–4, 30:22–24. [5] An investigation into General DSAZ, using the contact information gleaned from the airbill, revealed that ***543** it was linked to another company in Iran dealing with "industrial parts and things of that nature." *Id.* at 12:8–12.

[5] Rashti has been indicted as a coconspirator in this case under the name Arash Rashti Mohammad, *see* Second Superseding Indictment, ECF No. 95, but because Rashti is an Iranian national currently located in Iran, *id.* ¶ 5, the United States has not been able to acquire jurisdiction over him or to bring him before a judicial officer of this Court.

Shortly thereafter on March 29, 2012, Baird conducted interviews with individuals at a company called Geiger Pumps, which confirmed that it had sold two cyclone separators to Saboonchi based on his representation that "the end user was domestic use only." *Id.* at 12:13–22. Baird also noted that the airbill had listed the value of the cyclone separators as $100 but that their actual value was over $2,100. *Id.* at 15:21–16:2. Although reporting requirements only apply to items worth at least $2,500, Baird testified, based upon her training and experience, that "when people tend to undervalue stuff, it's to keep things below the radar." *Id.* at 16:6–8. On March 30, 2012, Baird conducted interviews with another supplier, RG Group, from which Saboonchi also had made purchases. *Id.* at 12:23–13:4, 31:9–20. Somewhere around this time, Baird caused Saboonchi's information to be entered into TECS as a person of interest. *Id.* at 4:7–11.[6] Also based on her investigation, Baird testified that when she was contacted by Burkhardt, she asked him to detain Saboonchi's electronic media and to search his vehicle to take advantage of the Government's border search authority. *See id.* at 5:6–9; 33:4–14.

[6] Although it is not entirely clear that the reason why Saboonchi was flagged in the TECS database is relevant to determining whether CBP agents acted permissibly in relying on the database, *see Herring v. United States,* 555 U.S. 135, 129 S.Ct. 695, 172 L.Ed.2d 496 (2009) (recognizing good-faith exception to exclusionary rule even where search resulted from police negligence), to the extent that Baird's entry in TECS was based on reasonable, articulable suspicion, it obviates the need to analyze the good faith of the officials involved.

With respect to the Devices, Baird testified that she received them in a FedEx package from Agent O'Rourke and immediately handed them over to her computer forensics agent, Agent Mycel. Baird Tr. 7:21–8:1. Baird told O'Rourke not to examine the Devices and had not examined them herself, so that she could give them to a specialist in the preservation of computer evidence. *See id.* at 8:22–9:10. Images were made of the hard drives of both phones and of the USB drive, but the image of the Sony phone later was deleted after it was determined that it was not Saboonchi's. *Id.* at 24:7–25:6. Among the files that were searched, Baird found evidence of telephone contact with an employee of Geiger Pumps and a copy of Saboonchi's résumé that showed that he had interned with an Iranian company. *Id.* at 15:11–20.

On April 13, 2012, after the Devices had been imaged, Baird arranged for Saboonchi to come to the U.S. Custom House in Baltimore so that she could return the Devices to him. *Id.* at 20:20–22. Saboonchi pulled his car up outside the Custom House, and Baird and another agent came out to meet him. *Id.* at 20:21–23. In addition to turning over the devices, Baird asked Saboonchi whether he was aware of the sanctions in place with respect to Iran and Saboonchi responded that he was aware that there were some restrictions in place, that he knew people who had had difficulties receiving money from family in Iran, and that he believed that United States residents were not permitted to use Iranian airlines. *Id.* at 21:2–15. Baird advised Saboonchi that he would need to get permission from the Office of Foreign Asset Control ("OFAC") if he wished to conduct business with entities in Iran. *Id.* at 21:16–24. Baird also asked questions about Saboonchi's internship with an Iranian company but did not ask if he was ***544** exporting products to Iran. *Id.* at 38:14–40:7. Saboonchi asked Baird why his wife had not received her Permanent Resident Card and Baird offered to look into it, taking down Saboonchi's wife's information to aid in her inquiry. *Id.* at 22:23–23:1.

The entire interaction between Baird and Saboonchi took place on the street, at Saboonchi's car. *Id.* at 20:20–23. Although Baird was carrying a weapon, it was concealed, *id.* at 22:10–12, and Baird testified that Saboonchi was free to leave at any time, *id.* at 22:13–16.

C. Supplemental Briefing

At the conclusion of the hearing, I resolved the Fifth Amendment issue, finding that neither the initial questioning of Saboonchi by CBP nor his conversation with Special Agent Baird were custodial for the purposes of *Miranda,* relying in part upon *United States v. FNU LNU,* 653 F.3d 144, 153–54 (2d Cir.2011) (noting that the likelihood that those entering the country expect some degree of confinement and questioning reduces the

likelihood that such restrictions would be perceived as custodial); *see also* Hr'g Tr., Argument and Rulings (the "Ruling Tr."), 14:19–19:1. [7]

[7] Saboonchi now has changed counsel and his new attorney has filed a Motion to Suppress Statements, ECF No. 110, asserting, *inter alia,* Fifth Amendment violations arising out of the April 13, 2013 encounter. *Id.* ¶ 2(b). Though similar issues were addressed at the motions hearing, nothing herein is intended to relate to the resolution of the merits of Saboonchi's new motion to suppress.

With respect to the seizure [8] and subsequent search of the Devices, I found that current state of the law provides considerably less clarity. Although it seemed that the seizure of Saboonchi and the Devices was supported by reasonable suspicion, the Government had taken the position that its actions constituted a routine border search for which no suspicion was required, Gov't Opp'n 26–29, and I noted that the nature and extent of the authority to image and forensically search those devices was unclear. *See* Ruling Tr. 31:4–20. Because this is an unsettled area of the law, and one that increasingly is important as ever greater aspects of our lives involve the use of digital devices, I stated my intention to issue a written opinion setting forth the reasons for my decision. *Id.* at 36:25–37:14.

[8] CBP and HSI attempt to distinguish between a "detention" and a "seizure." *See* Burkhardt Tr. 57:16–17 ("I don't mean to get technical, but CBP does not seize, we detain."); *see also* U.S. Dep't of Homeland Sec., *Privacy Impact Assessment for the Border Searches of Electronic Devices* 5 (Aug. 25, 2009), *available at* http://www.dhs. gov/xlibrary/assets/privacy/privacy_pia_cbp_laptop.pdf (defining a "detention" as "a temporary detention of the device during an ongoing border search" and "seizure" as occurring only "when CBP or ICE determines there is probable cause to believe a violation of law ... has occurred"). As explained on the record, however CBP and HSI may choose to characterize their actions, it was a constitutional seizure "the minute [the Devices were] taken," so that this distinction is not relevant for purposes of the Fourth Amendment. *See* Ruling Tr. 30:10–19.

The Government requested, and I granted, the opportunity to provide supplemental briefing in light of the importance of the issue and the paucity of other opinions addressing it. *See id.* at 40:11–41:4. That briefing now has been completed, *see* Gov't Supp. Mem., ECF No. 87; Def.'s Resp. Mem., ECF No. 90, and I can turn now to addressing the issues raised in Defendant's motion.

II. THE BORDER SEARCH DOCTRINE

A. Types of Border Searches

[1] **[2]** Any analysis of a border search must begin from the proposition that ***545** "[t]he Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border." *United States v. Flores–Montano,* 541 U.S. 149, 152, 124 S.Ct. 1582, 158 L.Ed.2d 311 (2004). It therefore is well-established "[t]hat searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border." *United States v. Ramsey,* 431 U.S. 606, 616, 97 S.Ct. 1972, 52 L.Ed.2d 617 (1977). "Routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant ...." *United States v. Montoya de Hernandez,* 473 U.S. 531, 538, 105 S.Ct. 3304, 87 L.Ed.2d 381 (1985).

[3] **[4]** **[5]** But even at the border, the Fourth Amendment continues to protect against *unreasonable* searches and seizures; the only difference is that, at the border, routine searches become reasonable because the interest of the Government is far stronger and the reasonable expectation of privacy of an individual seeking entry is considerably weaker. *See Carroll v. United States,* 267 U.S. 132, 154, 45 S.Ct. 280, 69 L.Ed. 543 (1925) ("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."). *But cf. United States v. Verdugo–Urquidez,* 494 U.S. 259, 274–75, 110 S.Ct. 1056, 108 L.Ed.2d 222 (1990) (holding that the Fourth Amendment does not apply to non-citizens searched or seized outside of the United States). When a search stretches beyond the routine, it must rest on reasonable, particularized suspicion, *Montoya de Hernandez,* 473 U.S. at 541, 105 S.Ct. 3304, which is significantly less demanding than the showing of probable cause required

to secure a warrant for a domestic search, *see* U.S. Const. amend. IV. It is not so easy to divine precisely where a border search falls along the continuum from reasonable to unreasonable, particularly when the search involves imaging the entire contents of two smartphones and a flash drive.

The Supreme Court has not addressed the issue often, but it has laid out the broad strokes of what constitutes a routine, versus a nonroutine, search. On the one hand, in *United States v. Flores–Montano,* the Court held that "the Government's authority to conduct suspicionless inspections at the border includes the authority to remove, disassemble, and reassemble a vehicle's fuel tank." 541 U.S. at 155, 124 S.Ct. 1582. In so holding, the Court found that the privacy interest in the contents of a person's gas tank was less than that in the contents of a passenger compartment, that such searches were relatively brief, and that the possibility of permanent damage to a car was so remote that it did not implicate a legitimate property interest, particularly because an owner of a damaged car might be entitled to recover damages. *Id.* at 154–55, 124 S.Ct. 1582 (citing *Carroll,* 267 U.S. at 154, 45 S.Ct. 280).

On the other hand, *United States v. Montoya de Hernandez* presents an extreme factual situation that clearly exceeded a mere routine search or seizure, in which a defendant suspected of smuggling drugs in her alimentary canal was told that she would not be released into the United States until she submitted to an x-ray or "produced a monitored bowel movement that would confirm or rebut the inspectors' suspicions." 473 U.S. at 534–35, 105 S.Ct. 3304. As a result, she "was detained incommunicado ***546** for almost 16 hours before inspectors sought a warrant." *Id.* at 542, 105 S.Ct. 3304. In holding that the detention required, and in that particular case was justified by, reasonable suspicion, *id.* at 541, 105 S.Ct. 3304, the Court expressly refrained from defining "what level of suspicion, if any, is required for nonroutine border searches such as strip, body cavity, or involuntary x-ray searches," *id.* at 541 n. 4, 105 S.Ct. 3304.

[6] The principal case on border searches in the Fourth Circuit is *United States v. Ickes,* 393 F.3d 501 (4th Cir.2005), which, like this case, dealt with a computer search—although not a forensic examination of an identical image of the entire contents of the computer's hardware. In *Ickes,* the defendant was selected for secondary inspection at the U.S.—Canadian border because the large amount of property he had in his van seemed inconsistent with his claim that he was returning from a vacation. *Id.* at 502. In a routine secondary inspection, the inspector found a video camera with "a tape of a tennis match which focused excessively on a young ball boy." *Id.* The agents searched the van more thoroughly and turned up marijuana seeds and pipes, a copy of a Virginia warrant for Ickes's arrest, and "several albums containing photographs of provocatively-posed prepubescent boys, most nude or semi-nude." *Id.* at 503. The Customs agents placed Ickes under arrest but continued to search the van, discovering a computer and approximately seventy-five disks containing child pornography. *Id.* The Fourth Circuit concluded that the search was a routine border search that did not require a showing of reasonable suspicion, *id.* at 505–06, even though the officers likely had reasonable suspicion before they viewed the contents of the disks. Thus under *Ickes,* the mere fact that a search includes computer files does not transform it from routine to nonroutine.

B. Location of Border Searches

[7] **[8]** A border search need not take place *at* the border—indeed, here it appears that Saboonchi's Devices were seized at a border but actually were searched in Baltimore, well within the territory of the United States. Courts have recognized two different ways that a search may fall within the border search doctrine even though it does not occur at a physical border. First, border searches "may in certain circumstances take place not only at the border itself, but at its functional equivalents as well." *Almeida–Sanchez v. United States,* 413 U.S. 266, 272, 93 S.Ct. 2535, 37 L.Ed.2d 596 (1973). The "functional equivalent" of a border may include "an established station near the border, at a point marking the confluence of two or more roads that extend from the border," or the search of passengers and cargo arriving at an airport within the United States after a nonstop flight from abroad. *Id.* at 273, 93 S.Ct. 2535. As these locations are the functional equivalent of a border, the analysis is no different from a search at an actual, physical border and no additional suspicion is required. *See id.*

[9] **[10]** Second, courts have permitted " 'extended border searches,' under which 'border' is given a geographically flexible reading within limits of reason related to the underlying constitutional concerns to

protect against unreasonable searches." *United States v. Bilir,* 592 F.2d 735, 740 (4th Cir.1979). "[T]he 'extended border search' doctrine has been applied to entry border searches conducted some time after the border was crossed." *United States v. Cardona,* 769 F.2d 625, 628 (9th Cir.1985) (citing *United States v. Caicedo–Guarnizo,* 723 F.2d 1420, 1422 (9th Cir.1984)). An extended border search may be necessary ***547** because the first contact with a customs official occurs away from the border, or because officers have elected to allow a suspect to pass through the border in order to perform a search at a later time. *Bilir,* 592 F.2d at 740. Unlike searches that actually occur at a border or the functional equivalent thereof, an extended border search requires reasonable suspicion with respect to the criminal nature of the person or thing searched as well as reasonable suspicion that the subject of the search has crossed a border "within a reasonably recent time." *Id.*

III. DISCUSSION

At the outset, it is important to understand what takes place during a forensic computer search, and what distinguishes it from what may usefully be regarded as a "conventional" search of a computer or digital device. Though every search is different, a forensic search has certain hallmarks by which it can be identified. First, "the computer forensics process always begins with the creation of a perfect 'bitstream' copy or 'image' of the original storage device saved as a 'read only' file." Orin S. Kerr, *Searches and Seizures in a Digital World,* 119 Harv. L.Rev. 531, 540 (2005). Then, a computer forensics expert will use specialized software to comb through the data, often over the course of days, weeks, or even months, *id.* at 537–38, searching the full contents of the imaged hard drive, examining the properties of individual files, and probing the drive's unallocated "slack space" to reveal deleted files, *id.* at 542–43. Although directed by a forensic examiner, an integral part of a forensic examination is the use of technology-assisted search methodology, where the computer searches vast amounts of data that would exceed the capacity of a human reviewer to examine in any reasonable amount of time. The techniques used during a forensic search can be distinguished from a conventional computer search, in which a Customs officer may operate or search an electronic device in much the same way that a typical user would use it.

As I will explain, a conventional computer search can be deeply probing and, much like any search of personal effects at the border, has the potential to be invasive. Yet these concerns do not bring a conventional computer search outside of the broad authority granted under the border search doctrine any more than a suitcase is immunized from search because it may contain a personal diary. Despite the vast amounts of data available in an electronic device, a conventional search is limited by the amount of time one Customs officer has to devote to reviewing the contents of digital evidence at the border while its owner awaits the outcome of the search. Even if that review may take a matter of hours, the amount of data searched will be a mere fraction of what is on the device, given the storage capacity of modern electronic devices. And in any event, though such a search may last hours, it will not last days. There is only so much time that a Customs officer has to devote to the border search of a computer. 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.

In contrast, a forensic examination of a computer or other electronic device using sophisticated technology-assisted search methodologies can exceed vastly the capacity of a human searching and viewing files. Moreover, this type of search exposes a class of data that raises novel privacy concerns, including files that a user had ***548** marked as "deleted" [9] and location data that may provide information about activities in the home and away from the border. For this reason, a forensic search of an electronic device differs significantly from a conventional search not merely in degree, but in kind. Accordingly, as explained below, a forensic search of an electronic device seized at the border cannot be performed absent reasonable, articulable suspicion.

9 The mere act of marking a file as "deleted" does not actually delete it from a computer; rather, it merely removes references to the file from the computer's Master File Table, which marks the data clusters where the file is located as available for future use. The file itself will remain until those clusters actually are overwritten or are "zeroed out" so as to remove the file itself from the computer. Kerr, *supra,* at 542–43.

A. Analytical Framework

[11] The framework established by the Supreme Court and the Fourth Circuit allows for three possible ways to

analyze the seizure and search of Saboonchi's Devices. The Government has taken the position that the detention, seizure, imaging, and forensic search of the Devices should be viewed as a routine border search, so that no suspicion was required and the search clearly was permissible under any facts. Gov't Opp'n 26. Saboonchi has argued that, because the actual search of the Devices took place at a field office in Baltimore, several hundred miles from where Saboonchi crossed the border, it is best viewed as an extended border search for which reasonable suspicion was required. Def.'s Reply 2. In the alternative, Saboonchi argues that, unlike a conventional search of a digital device such as viewing a video or booting up a computer at the border, the act of seizing and imaging an electronic device and thereafter—perhaps days or weeks later—performing a forensic search crosses the line from a routine search to a nonroutine search, and therefore requires reasonable suspicion irrespective of where it is performed. *Id.* at 2, 5–6.

The facts here are distinct from cases that found an extended border search had occurred. In *United States v. Bilir,* for example, DEA agents declined to act immediately on information that heroin was concealed on a Turkish ship that would be entering several American ports, and instead followed the ship from port to port in hopes of apprehending the suspects. 592 F.2d 735, 737 (4th Cir.1979). The agents allowed the suspects to debark the ship in Baltimore in order to follow them, and the suspects eventually were stopped and searched at Baltimore Penn Station. *Id.* at 738. The Fourth Circuit upheld the search as an extended border search. *Id.* at 739. Similarly, in *United States v. Guzman–Padilla,* 573 F.3d 865 (9th Cir.2009), a Border Patrol agent used a controlled tire deflation device to stop a vehicle that already was in the United States but that the agent reasonably believed had entered the United States recently from Mexico. *Id.* at 875. Although it did not need to decide the issue, the Ninth Circuit noted that this might qualify as an extended border search. *Id.* at 877–78. In both of these cases, no search or seizure took place until after the suspects had cleared the border and were within the United States.

[12] The searches of the Devices in this case cannot be an extended border search because Saboonchi was not allowed to bring them across the border. *See United States v. Stewart,* 729 F.3d 517, 525 (6th Cir.2013) (finding no extended border search under similar circumstances "because [defendant's] laptop computers never cleared the border"). The seizure of the Devices occurred at the border itself. ***549** They then were shipped to Baltimore and were transferred from CBP to HSI, both of which play a role in securing the border. And once the devices were cleared for entry, they were returned, in Baltimore, to Saboonchi. "A border search of a computer is not transformed into an extended border search simply because the device is transported and examined beyond the border." *United States v. Cotterman,* 709 F.3d 952, 961 (9th Cir.2013). Thus, I find that this was not an extended border search; to the contrary, Saboonchi's Devices were not permitted to enter into the United States until they were returned to him in Baltimore, and any searches of those devices were pursuant to the general border search doctrine.

[13] Therefore, the level of suspicion required depends on whether the forensic search of the Devices was a routine search or a nonroutine search. Although I hold that a forensic search of a computer or electronic device should be considered a nonroutine search for which reasonable suspicion is required, I do so only after thorough analysis of the relevant law and factual considerations.

B. Routine Versus Nonroutine Searches Generally

Unsurprisingly, the overwhelming majority of searches that one would expect to encounter at the border fall into the category of conventional, routine border searches. This includes pat-downs, pocket-dumps, and even searches that require moving or adjusting clothing without disrobing, and also may include scanning, opening, and rifling through the contents of bags or other closed containers. But a routine search also may go beyond what a traveler otherwise may consider routine. For example, a routine search may extend to the inside of an automobile gas tank, *United States v. Flores–Montano,* 541 U.S. 149, 155, 124 S.Ct. 1582, 158 L.Ed.2d 311 (2004), to the contents of photograph albums or information encoded on video tapes, *United States v. Ickes,* 393 F.3d 501, 502–03 (4th Cir.2005), or to password protected or locked items, *United States v. McAuley,* 563 F.Supp.2d 672, 678 (W.D.Tex.2008). Insofar as the "touchstone of the Fourth Amendment is reasonableness," *Florida v. Jimeno,* 500 U.S. 248, 250, 111 S.Ct. 1801, 114 L.Ed.2d 297 (1991) (citing *Katz v. United States,* 389 U.S. 347, 360, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967)), it does not require Napoleonic insight to see how the power to conduct

searches of this kind on a routine basis, without suspicion, is the *sine qua non* of customs and border enforcement; otherwise there would be nothing to stop travelers or commercial shippers from dodging our customs laws with impunity so long as they avoid drawing attention. *See, e.g., United States v. Johnson,* 991 F.2d 1287, 1292 (7th Cir.1993) ("A customs official might have to rummage through any border entrant's luggage to ascertain whether all items have been declared properly.").

A wide range of searches of persons also have been upheld as routine even if they involve some level of indignity or intrusiveness, so long as they fall short of a strip search and do not expose the cavities of the body. *See, e.g., Bradley v. United States,* 299 F.3d 197, 203 (3d Cir.2002) (holding that patdowns are routine searches that do not require reasonable suspicion); *United States v. Kelly,* 302 F.3d 291, 294–95 (5th Cir.2002) (dog sniff was a routine border search even where dog made brief contact with suspect's groin); *United States v. Charleus,* 871 F.2d 265, 266–67 (2d Cir.1989) (touching defendant's back and, upon discovering a bump, lifting the back of his shirt was a routine search); *United States v. Brown,* 499 F.2d 829, 833 (7th Cir.1974) (lifting an ***550** ankle-length skirt to just above a female suspect's knees in a room with only women constituted a routine search).

[14] **[15]** On the other hand, *United States v. Ramsey* left open the possibility that "a border search might be deemed 'unreasonable' because of the particularly offensive manner in which it is carried out." 431 U.S. 606, 618 n. 13, 97 S.Ct. 1972, 52 L.Ed.2d 617 (1977). For example, there is a general consensus that even the border search power cannot justify a strip search without any particularized suspicion. *See, e.g., Montoya de Hernandez,* 473 U.S. at 541 n. 4, 105 S.Ct. 3304 (listing a category of "nonroutine border searches" including a strip or body cavity search); *United States v. Rodriguez,* 592 F.2d 553, 556 (9th Cir.1979) ("While anyone at a border may be stopped for questioning and subject to an inspection of luggage, handbags, pockets, wallets, without any suspicion at all on the part of customs officials, 'real suspicion' is required before a strip search may be conducted ...." (citations omitted)); *United States v. Asbury,* 586 F.2d 973, 975–76 (2d Cir.1978) (a strip search is "such an extensive invasion of privacy, [a border official] should have a suspicion of illegal concealment that is based upon something more than the border crossing, and the suspicion should be substantial enough to make the search a reasonable exercise of authority"); *United States v. Himmelwright,* 551 F.2d 991, 994–95 (5th Cir.1977) (holding that reasonable suspicion, but nothing more, is required to justify a strip search at the border). "[A] border search that goes beyond the routine is nevertheless justified merely by reasonable suspicion, a lesser standard than required for analogous non-border searches." *United States v. Oriakhi,* 57 F.3d 1290, 1297 (4th Cir.1995) (citing *Montoya de Hernandez,* 473 U.S. at 541, 105 S.Ct. 3304).

Courts have struggled to define a clear dividing line between routine and nonroutine searches. In *United States v. Braks,* 842 F.2d 509 (1st Cir.1988), the First Circuit listed the following relevant factors:

> (i) whether the search results in the exposure of intimate body parts or requires the suspect to disrobe;
>
> (ii) whether physical contact between Customs officials and the suspect occurs during the search;
>
> (iii) whether force is used to effect the search;
>
> (iv) whether the type of search exposes the suspect to pain or danger;
>
> (v) the overall manner in which the search is conducted; and
>
> (vi) whether the suspect's reasonable expectations of privacy, if any, are abrogated by the search.

842 F.2d at 512 (footnotes omitted). These factors did not represent "an exhaustive list of equally-weighted concerns," and each search was a fact-specific inquiry in which those factors were among the relevant considerations. *Id.* at 513.

Other courts have focused specifically on familiar touchstones such as the exposure of intimate body parts and details, as well as a suspect's reasonable expectations of privacy. In *United States v. Vega–Barvo,* 729 F.2d 1341 (11th Cir.1984), the Eleventh Circuit, considering the permissibility of an x-ray search of a person, observed:

> To determine the "intrusiveness" level of the internal body searches involved in today's cases, it is necessary to decide whether intrusiveness is to be defined in terms of whether one search

> will reveal more than another, or whether intrusiveness is to be interpreted in terms of the indignity that will be suffered by the person being searched. For example, is an x-ray more intrusive than a cavity search because it will reveal more than ***551** the cavity search, or less intrusive because it does not infringe upon human dignity to the same extent as a search of private parts? A person can retain some degree of dignity during an x-ray, but it is virtually impossible during a rectal probe, despite the more limited scope of such a search.

Id. at 1345. Although the Eleventh Circuit held that the true touchstone is "personal indignity," *id.* at 1346, the distinction did not seem to make much difference, as the Eleventh Circuit held that an x-ray search is "more intrusive than a frisk, [though] no more intrusive than a strip search," and therefore required reasonable suspicion, but not more, *id.* at 1349. The Supreme Court and the Fourth Circuit also have assumed, but not decided, that an x-ray search is nonroutine. *See Montoya de Hernandez,* 473 U.S. at 541 n. 4, 105 S.Ct. 3304; *United States v. Aguebor,* 166 F.3d 1210, 1999 WL 5110, at *3 (4th Cir. Jan. 4, 1999). Courts also have found searches to be nonroutine where they required the removal of an artificial limb, *United States v. Sanders,* 663 F.2d 1, 3–4 (2d Cir.1981), or required a woman partially to disrobe to display her girdle, *United States v. Palmer,* 575 F.2d 721, 723 (9th Cir.1978). But in each of these cases, the search was upheld as supported by reasonable suspicion. *Aguebor,* 1999 WL 5110, at *3; *Sanders,* 663 F.2d at 3–4; *Palmer,* 575 F.2d at 723.

Though most of these cases deal with searches of persons, some searches of property also have been found to be nonroutine. In *Flores–Montano,* the Supreme Court noted —and declined to comment on—a series of cases finding that "exploratory drilling searches" required reasonable suspicion. *See Flores–Montano,* 541 U.S. at 154 n. 2, 124 S.Ct. 1582; *see also United States v. Rivas,* 157 F.3d 364, 366–67 (5th Cir.1998) (reasonable suspicion required to drill into frame of truck trailer); *United States v. Robles,* 45 F.3d 1, 5 (1st Cir.1995) (reasonable suspicion was required to drill into a "closed, metal cylinder"); *United States v. Carreon,* 872 F.2d 1436, 1440–41 (10th Cir.1989) (reasonable suspicion required to drill hole into wall of camper). The Supreme Court noted that such searches are "potentially destructive" and could be considered " 'particularly offensive' " and therefore nonroutine. *See Flores–Montano,* 541 U.S. at 154 n. 2, 124 S.Ct. 1582 (quoting *Ramsey,* 431 U.S. at 618 n. 13, 97 S.Ct. 1972). It is not difficult to see how these searches, involving both physical damage to property and the invasion of a space that may contain private material, can be analogized to body cavity searches.

[16] There also is a line of cases that has held that searches of private quarters on ships arriving at U.S. ports from abroad resemble the search of a home too closely to be permitted absent reasonable suspicion. In *United States v. Whitted,* customs officials entered the defendant's cabin after a query on a ship's manifest against TECS returned a "one-day lookout" for the defendant. 541 F.3d 480, 483 (3d Cir.2008). When the defendant challenged the search, the Third Circuit found that the cabin of a ship presents the intersection of two opposed but important values: the broad authority of the sovereign to perform searches on those entering the country, and the heightened protection the Fourth Amendment provides for one's home. *Id.* at 488. The court held that reasonable suspicion—but no more—was required for such a search because the "high expectation of privacy and level of intrusiveness" brought it beyond the routine. *Id.* at 489; *see also id.* at 486–87 (" 'something more than naked suspicion' " required to search a ship's cabin (quoting *United States v. Alfonso,* 759 F.2d 728, 738 (9th Cir.1985)); *United States v. Cunningham,* ***552** No. 96–265, 1996 WL 665747, at *3 (E.D.La. Nov. 15, 1996) (reasonable suspicion required to search private areas of a ship); *State v. Logo,* 798 So.2d 1182, 1183 (La.Ct.App.2001) (reasonable suspicion required to search passenger's cabin on ship). Accordingly, even if a search is not destructive or damaging, if it is sufficiently invasive or intrusive, or butts up against other Fourth Amendment values, it may be nonroutine in any event.

C. Prior Case Law on Searches of Electronic Media

[17] *Ickes* makes it clear that a routine border search may include a conventional inspection of electronic media and a review of the files on them just as it may include physical papers. *See Ickes,* 393 F.3d at 505–06. Furthermore, *Ickes* comports with the clear weight of precedent from

other courts. *See, e.g., United States v. Arnold,* 533 F.3d 1003, 1008 (9th Cir.2008) ("reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border"); *United States v. Linarez–Delgado,* 259 Fed.Appx. 506, 508 (3d Cir.2007) (viewing a videotape in defendant's possession was permissible as part of a routine border search); *United States v. Bunty,* 617 F.Supp.2d 359, 365 (E.D.Pa.2008) (viewing files on defendant's floppy disk permissible as part of suspicionless border search). In these cases, courts have analogized a laptop to a closed container that may be opened and its contents searched at the border. *See Arnold,* 533 F.3d at 1007.

But courts have disagreed on whether the same principles apply to forensic searches of electronic devices. There have been two recent opinions addressing the issue in the past year, *United States v. Cotterman,* 709 F.3d 952 (9th Cir.2013) (en banc), and *Abidor v. Napolitano,* 990 F.Supp.2d 260, 2013 WL 6912654 (E.D.N.Y. Dec. 31, 2013), that reached opposite conclusions. Moreover, neither *Cotterman* nor *Abidor* is, by itself, sufficiently persuasive to resolve the issue under Fourth Circuit law.

United States v. Cotterman is the first (and as far as I have found, the only) circuit court case to address the issue, and it held that a forensic search of electronic media could not be a routine search. 709 F.3d 952. Cotterman was returning to the country from a vacation in Mexico when, during primary inspection at the border, a search of TECS returned a hit for Cotterman indicating that he was a sex offender. *Id.* at 957. The border agents called the contact person listed in the TECS entry and, as a result, came to believe that Cotterman was involved " 'in some type of child pornography.' " *Id.* On secondary inspection, Cotterman was found to have two laptop computers and three digital cameras, which contained personal photographs and several password-protected files. *Id.* at 957–58.

Immigration and Customs Enforcement ("ICE") agents arrived at the border crossing, Mirandized Cotterman and his wife, and interrogated them. *Id.* at 958. Cotterman offered to help them access the files on his computer, but the ICE agents declined out of concerns that he would delete the files or that his laptop was " 'booby trapped.' " *Id.* Eventually the Cottermans were allowed to leave but the ICE agents retained the laptop computers and a digital camera, which they transported 170 miles to an ICE Computer Forensic Examiner. *Id.* The examiner imaged and performed forensic searches of the hard drives of the electronic devices and found seventy-five images of child pornography hidden in the unallocated space on Cotterman's laptop. *Id.* He contacted the Cottermans shortly thereafter and informed ***553** Cotterman that he would need assistance to access certain password-protected files; Cotterman responded that he would need to track down the passwords but instead he fled the country without meeting with ICE officials. *Id.* at 958–59.

The Ninth Circuit found no problem with the initial search of Cotterman's devices at the border itself, *id.* at 960, but held that "the comprehensive and intrusive nature of a forensic examination ... trigger[s] the requirement of reasonable suspicion here," *id.* at 962, because the material that can be gleaned from a forensic search of an electronic device differed not only in quantity, but in kind, from that which previously had been upheld. The Ninth Circuit explained:

> The private information individuals store on digital devices—their personal "papers" in the words of the Constitution—stands in stark contrast to the generic and impersonal contents of a gas tank....
>
> The amount of private information carried by international travelers was traditionally circumscribed by the size of the traveler's luggage or automobile. That is no longer the case. Electronic devices are capable of storing warehouses full of information....
>
> The nature of the contents of electronic devices differs from that of luggage as well. Laptop computers, iPads and the like are simultaneously offices and personal diaries. They contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails. This type of material implicates the Fourth Amendment's specific guarantee of the people's right to be secure in their "papers." ...
>
> Electronic devices often retain sensitive and confidential information far beyond the perceived point of erasure, notably in the form of browsing histories and records of deleted files. This quality makes it impractical, if not impossible, for individuals to make meaningful decisions regarding what digital content to expose to the scrutiny that accompanies international travel. A person's digital life ought not be hijacked simply by

> crossing a border. When packing traditional luggage, one is accustomed to deciding what papers to take and what to leave behind. When carrying a laptop, tablet or other device, however, removing files unnecessary to an impending trip is an impractical solution given the volume and often intermingled nature of the files. It is also a time-consuming task that may not even effectively erase the files.
>
> ....
>
> ... Such a thorough and detailed search of the most intimate details of one's life is a substantial intrusion upon personal privacy and dignity. [The Ninth Circuit therefore held] that the forensic examination of Cotterman's computer required a showing of reasonable suspicion, a modest requirement in light of the Fourth Amendment.

Id. at 964–65, 968 (internal citations omitted). But the court took pains to note that suspicionless conventional (that is to say, nonforensic) searches of electronics still would continue, and that "[r]easonable suspicion leaves ample room for agents to draw on their expertise and experience to pick up on subtle cues that criminal activity may be afoot." *Id.* at 967 (citing *United States v. Tiong,* 224 F.3d 1136, 1140 (9th Cir.2000)). Finding that there was reasonable suspicion with respect to Cotterman, the Ninth Circuit majority upheld the forensic search of Cotterman's electronic devices. *Id.* at 970.

It is difficult to rely on *Cotterman* as setting forth a rule of general applicability. ***554** First, the Ninth Circuit begins with the proposition that the border search doctrine is " 'a narrow exception to the Fourth Amendment prohibition against warrantless searches without probable cause.' " *Id.* at 960 (quoting *United States v. Seljan,* 547 F.3d 993, 999 (9th Cir.2008) (en banc)). But the Fourth Circuit cases, which are binding on this Court, have stated in clear terms that even if the border search doctrine is narrow in its geographical scope (that is, confined to the border or its functional equivalents), it provides "broad authority to conduct border searches." *Ickes,* 393 F.3d at 506. Accordingly, even were I to adopt *Cotterman's* reasoning *in toto,* I would be required independently to assess whether its conclusion comported with Fourth Circuit law.

Further, it is difficult to figure out the precise basis on which the Ninth Circuit distinguished forensic searches from conventional ones. The court's main rationale seemed to be that "the uniquely sensitive nature of data on electronic devices carries with it a significant expectation of privacy and thus renders an exhaustive exploratory search more intrusive than with other forms of property." *Cotterman,* 709 F.3d at 966. But *Cotterman* seemed to avoid laying down a distinction between forensic searches and intrusive but conventional ones, instead deferring to "the ability of law enforcement to distinguish a review of computer files from a forensic examination." *Id.* at 967. Judge Callahan, concurring in the result but disputing the *en banc* majority's reasoning, suggests that the holding "relies primarily on the notion that electronic devices are special," and therefore the reasoning in *Cotterman* cannot be squared with the Fourth Circuit's holding that "electronic devices are like any other container that the Supreme Court has held may be searched at the border without reasonable suspicion." *Id.* at 973, 975 (Callahan, J., concurring in part, dissenting in part, and concurring in the judgment) (discussing *Ickes,* 393 F.3d 501). And Judge Smith, writing in dissent, goes even further in suggesting that "[m]apping our privacy rights by the amount of information we carry with us leads to unreasonable and absurd results," such as rendering "a Mini Cooper filled with documents [ ] entitled to less privacy protection at the border than a stretch Rolls–Royce filled with documents." *Id.* at 987 (Smith, J., dissenting). At the very least, *Ickes* forecloses the possibility that the mere fact that an electronic device may contain massive amounts of personal data, by itself, can change the legal analysis at the border, *see Ickes,* 393 F.3d at 505–06, and were I to accept *Cotterman's* conclusion, I must do so on a basis other than that used by the Ninth Circuit.

If *Cotterman* raises complex and difficult questions as to its rationale and its consistency with Fourth Circuit law, *Abidor v. Napolitano* appears to lack precedential value—both because there are questions about the court's jurisdiction where it stated legal conclusions regarding the constitutionality of the searches after having determined that none of the plaintiffs had standing to challenge them, and because certain aspects of its reasoning are unpersuasive. *Abidor* was a civil suit brought by an individual plaintiff named Pascal Abidor, the National Association of Criminal Defense Lawyers, and the National Press Photographers Association. *Abidor v. Napolitano,* 990 F.Supp.2d 260, 2013 WL 6912654 (E.D.N.Y. Dec. 31, 2013). Abidor was an academic whose laptop computer and external hard drive were searched

and detained on an Amtrak train from Canada to the United States when CBP agents found photographs of Hezbollah and Hamas on his laptop; he alleged that his laptop and external drive had been searched and physically opened. ***555** *Id.* at 267–68, at *5. The association plaintiffs argued only that the possibility that their electronic devices could be searched in the absence of suspicion made it difficult for them to protect important, confidential information. *Id.* at 268–69, at *6. Importantly, the plaintiffs in *Abidor* sought only declaratory and injunctive relief. *Id.* at 263–64, at *1.

In *Abidor,* the court held that all plaintiffs lacked standing for the relief that they sought. *Id.* at 276–78, at *13–14.[10] But, in what appears to have been an exercise of "hypothetical jurisdiction," it opined that forensic searches may be performed without reasonable suspicion in any event.[11] *Abidor's* reasoning contains at least three analytical shortcomings: first, by designating the alternative to a "comprehensive forensic examination" to be a mere "quick look," *id.* at 269–70, at *7 (quoting *Cotterman,* 709 F.3d at 956, 960), *Abidor* obscures, rather than illuminates, the actual nature of the searches involved; second, *Abidor* fails to recognize the reality of the nature and role of digital devices in the contemporary world; and third, *Abidor* actually does not address forensic searches at all.

10 The court in *Abidor* held that "declaratory relief is not appropriate because it is unlikely that a member of the association plaintiffs will have his electronic device searched at the border, and it is far less likely that a comprehensive forensic search would occur without reasonable suspicion." 990 F.Supp.2d at 274, 2013 WL 6912654, at *11. With respect to Abidor himself, it also found that DHS already had deleted the images taken from his electronic devices. *Id.* "More significantly, however, [the court found it] difficult to understand how a threshold requirement of reasonable suspicion significantly alleviates the alleged harm that plaintiffs fear." *Id.* at 276, at *13. Noting that there was no claim for damages, the court held that the plaintiffs lacked standing for the declaratory relief they sought. *Id.* at 275–77, at *12–13.

11 The Supreme Court expressly has rejected the practice of " 'assuming' jurisdiction for the purpose of deciding the merits—the doctrine of 'hypothetical jurisdiction.' " *Steel Co. v. Citizens for a Better Env't,* 523 U.S. 83, 94, 118 S.Ct. 1003, 140 L.Ed.2d 210 (1998) (citation omitted). "Hypothetical jurisdiction produces nothing more than a hypothetical judgment —which comes to the same thing as an advisory opinion, disapproved by this Court from the beginning." *Id.* at 101, 118 S.Ct. 1003 (citing *Muskrat v. United States,* 219 U.S. 346, 362, 31 S.Ct. 250, 55 L.Ed. 246 (1911); *Hayburn's Case,* 2 U.S. (2 Dall.) 409, 1 L.Ed. 436 (1792)). Although *Abidor's* statements on forensic searches may amount to an advisory opinion, because of the paucity of other case law on the issue —and because of the sweeping statements made in *Abidor*—I consider its reasoning nevertheless even if it is not clear that it is precedential.

At the outset of its discussion of computer searches, *Abidor* defines the relevant distinction as between a "quick look," which is "only a cursory search that an officer may perform manually," and a "comprehensive forensic evaluation," which is "an exhaustive search of a computer's entire hard drive." *Id.* at 269–70, at *7 (citations omitted). This distinction purports to come out of *Cotterman,* but that is questionable. The phrase "quick look" appears only a single time in *Cotterman,* where the Ninth Circuit noted that it "ha[s] approved a quick look and unintrusive search of laptops," *Cotterman,* 709 F.3d at 960 (citing *United States v. Arnold,* 533 F.3d 1003, 1009 (9th Cir.2008)), and does not appear elsewhere in the border search case law. Moreover, in *United States v. Arnold,* the case that *Cotterman* described as involving a "quick look," the defendant was detained for several hours while his computer was searched thoroughly. 533 F.3d at 1009. This hardly is "quick" in the conventional sense and, to the contrary, actually shows how lengthy and comprehensive a conventional search can be. But by unnecessarily labeling a ***556** conventional computer search—which, under established law, may be quite extensive—as a "quick look," *Abidor* sets up a "quick look" as a straw man, creating a false dichotomy between a comprehensive forensic search and a cursory one that obviously will be insufficient in many instances to obtain the information justifiably needed to secure our borders.

Further, *Abidor's* reasoning seems to proceed from the view that, "it would be foolish, if not irresponsible, for plaintiffs to store truly private or confidential information on electronic devices that are carried and used overseas." *Abidor,* 990 F.Supp.2d at 277, 2013 WL 6912654, at *14. The court reasons that, because " 'the individual crossing a border is on notice that certain types of searches are likely to be made, ... he thus has ample opportunity to

diminish the impact of that search by limiting the nature and character of the effects which he brings with him.' " *Id.* at 280, at *16 (quoting 5 Wayne LaFave, *Search And Seizure: A Treatise of the Fourth Amendment* § 5(a) (4th ed.2011–12)).

While this reasoning may make sense with respect to non-digital "effects" carried by international travelers, it misperceives the reality of the capacity and use of digital devices in today's world: Portable electronic devices are ubiquitous. It neither is realistic nor reasonable to expect the average traveler to leave his digital devices at home when traveling. Over ninety percent of American adults own some kind of cellular phone and more than half of those own a smartphone—a category that includes, but is not limited to, iPhones, Android-based phones, and Blackberry devices. Aaron Smith, *Smartphone Ownership 2013,* PewResearch Internet Project (June 5, 2013), http://www. pewinternet.org/2013/06/05/ smartphone–ownership–2013. The public increasingly is attached to its phones: In 2010 the Pew Research Center found that sixty-five percent of adults—and seventy-two percent of parents—have slept with or near their phones. Amanda Lenhart, *Cell Phones and American Adults,* PewResearch Internet Project (Sept. 2, 2010), http://www.pewinternet. org/2010/09/02/cell-phones-and-american-adults/. Although many undoubtedly carry their phones as a convenience or a luxury, for others it is a necessity. Last year's ABA Legal Technology Resource Center's Technology Survey "reveals that 91% of all attorneys use a smartphone, and that percentage increases with the size of the law firm." *2013 ABA Tech Survey Once Again Shows Surge in Attorneys Using iPhone, iPad,* www.iphonejd.com/ iphone_jd/2013/07/2013–aba–tech–survey.html (July 30, 2013). In an increasingly global economy, professionals, businessmen, academics, and ordinary folk travel and maintain contact with family, friends, and colleagues at home while doing so. *See, e.g.,* Compl. ¶¶ 79–82, *Abidor v. Napolitano,* No. 10–4059 (E.D.N.Y. Sept. 7, 2010), 2010 WL 3477769 (attorneys allege they cannot work overseas without bringing electronic devices). And for travelers—whether for business or pleasure—who may leave behind children, sick or pregnant family members, or businesses and professions that depend upon them keeping current, the choice to travel without a reliable means of contact, in reality, is no choice at all.

Smartphones, in particular, have become so deeply embedded in day-to-day activities that travelers cannot reasonably be expected to travel without them, even if this were the only way to preserve their Fourth Amendment rights. For many users, smartphones completely have replaced alarm clocks and watches, cameras (both still and video), GPS devices, personal planners or datebooks, music players, newspapers, radios, and even books. *See* ***557** Brooke Crothers, *How Many Devices Can a Smartphone, Tablet Replace?* CNET (July 10, 2011 3:59 PM), http://news.cnet.com/8301–13924_3–20078244–64/ how-many-devices-can-a-smartphone-tablet-replace/. And as of 2012, eighteen percent of those who take digital photographs were using a smartphone as their primary camera, and that percentage has been growing as the percentage of people who use a dedicated camera for most of their photography has been falling. *See* Janice Chen, *CEA Says Phones Replacing Point–and–Shoot as Primary Photo Device,* ZDNet (Feb. 21, 2012 1:33 PM), http://www.zdnet.com/blog/digitalcameras/cea-says-phones-replacing-point-and-shoot-as-primary-photo-device/5616.

Encouraging Americans to travel without their electronic devices also is imprudent and leaves them exposed in the event of disaster abroad. In one recent incident, skiers caught in an avalanche were able to call for help using their cell phones and were rescued with help from a GPS unit. Mike Clarke, *3 Skiers Rescued from Avalanche near Hope, B.C.; Two Skiers Were Caught in the Avalanche, One Was Injured,* CBC News (Feb. 16, 2014 7:20 PM) (last updated Feb. 16, 2014 9:10 PM), http://www.cbc.ca/news/british–columbia–3–skiers–rescued–from–avalanche–near–hope–b–c–1.2539773. In another, an American family was able to use their cell phones to re-book hotels and flights (undoubtedly with substantial roaming fees) when they encountered problems with their reservations in the Dominican Republic. Douglass Dowty, *Forced Home After First Day of $4,600 Caribbean Vacation, Family Sues Travel Site* Hotwire.com, Syracuse.com (N.Y.) (Feb. 7, 2014 9:12 AM) (updated Feb. 7, 2014 1:06 PM), http://www.syracuse.com/news/index.ssf/2014/02/ clay_family_forced_home_after_ first_day_of_4600_caribbean_vacation_sues_booking.html. The Department of State expressly has recommended that travelers to certain regions enroll in the Smart Traveler Enrollment Program to receive "safety and security updates" and to ensure that those travelers

can be contacted in case of emergency—a goal that could not be accomplished if the travelers in question did not have electronic devices on which to receive updates and communications. *See, e.g.,* Bureau of Consular Affairs, *Russian Federation Travel Alert,* Dep't of State (updated March 14, 2014), http://travel.state. gov/content/passports/english/alertswarnings/russia-travel-alert-events-in-ukraine.html ("strongly recommend[ing] that U.S. citizens traveling to or residing in Russia enroll in the Department of State's Smart Traveler Enrollment Program"). And in the context of unrest in Ukraine, "the American Citizen Services Unit of the U.S. Embassy in Kyiv has implemented a text messaging network, whereby registered American citizens in Ukraine can receive short text messages ... providing important information in case of an emergency." *Travel Information by SMS Alerts,* Embassy of the United States, Kyiv, Ukraine, http://ukraine.usembassy.gov/announcements.html (last visited Apr. 4, 2014). It is likely that smartphones will become even more useful while traveling, as the ownership and use of smartphones abroad has been expanding rapidly. *See, e.g.,* Josh Heggestuen, *One in Every 5 People in the World Own a Smartphone, One in Every 17 Own a Tablet,* BusinessInsider.com (Dec. 15, 2013 3:23 PM), http://www.businessinsider.com/smartphone–and–tablet penetration–2013–10 (between 2009 and 2013, global smartphone ownership has expanded from 5% of the world's population to 22%, an increase of 1.3 billion smartphones).

Indeed, mobile devices now serve as digital umbilical cords to what travelers ***558** leave behind at home or at work, indispensable travel accessories in their own right, and safety nets to protect against the risks of traveling abroad and, particularly, of traveling to unstable or dangerous regions of the world. It therefore strikes me as unrealistic, if not unreasonable, to expect Americans traveling abroad to choose between leaving their devices at home or exposing them to the possibility of being imaged and forensically searched on reentry to this country without requiring Customs officers to articulate a justification even as modest as reasonable, articulable suspicion.

Finally, whereas *Cotterman* did not adequately explain why a forensic search differs from a conventional one, *Abidor* did not appear to recognize any meaningful distinction between the two at all.[12] But as explained below, there is a substantial difference between a conventional computer search and a forensic search.

12 It is worth noting that *Abidor* relied heavily on *Camara v. Municipal Court,* 387 U.S. 523, 87 S.Ct. 1727, 18 L.Ed.2d 930 (1967), which upheld a warrantless building inspection to enforce municipal codes, weighing the public interest served by such searches against the fact that the "inspections are neither personal in nature nor aimed at the discovery of evidence of crime." *Camara,* 387 U.S. at 537, 87 S.Ct. 1727. There is little question that border searches frequently are personal in nature; nor is there a genuine dispute that Saboonchi was searched in an attempt to disclose evidence of prior crimes, and not because his entry was believed to be a security threat in and of itself.

There are a handful of additional cases that, though decided in the shadow of forensic searches, did not directly address their permissibility. One notable circuit court case is *United States v. Stewart,* in which defendant Stewart was selected for secondary screening after being " 'standoffish' and 'confrontational' " towards CBP officers. 729 F.3d 517, 520 (6th Cir.2013). An officer booted up one of Stewart's two laptop computers and found "about a dozen thumbnail images ... that he believed to be child pornography." *Id.* at 521. At that time, an ICE agent was called in to assist; the agent detained the laptops but allowed Stewart to enter the country and board a flight to Maryland. *Id.* Later that day, an ICE forensic analyst searched the other computer (which had a dead battery and could not be booted up at the airport) by scrolling through it and located additional suspected child pornography. *Id.* At that time, ICE obtained a search warrant and a forensic examination of both computers was performed. *Id.*

Like the Fourth Circuit, the Sixth Circuit characterized the border search doctrine as "a broad exception to the Fourth Amendment's requirement of probable cause." *Id.* at 524. But because a warrant was obtained prior to any forensic search, the only question that was raised on appeal was whether the initial detention and conventional searches of Stewart's computers prior to obtaining the search warrant constituted an extended border search, requiring reasonable suspicion, or a routine border search, for which suspicion is not required. *See id.* The Sixth Circuit held that this was a routine search, noting that the second conventional search, though performed without a warrant, was "the same search that they could have

done the previous day had the proper equipment [*i.e.,* a computer charger] been present at the airport," and that the search occurred only one day later and twenty miles away. *Id.* at 525–26.

In *House v. Napolitano,* No. 11–10852–DJC, 2012 WL 1038816 (D.Mass. March 28, 2012), plaintiff House was an organizer of the Bradley Manning Support Network who alleged that he was targeted by various government agencies as a result of his ***559** support for Bradley Manning. *Id.* at *2.[13] When returning from a vacation in Mexico, House initially was cleared through customs at Chicago O'Hare International Airport, but was then approached in the terminal by DHS officials who detained him and demanded all of his electronics, including a laptop computer, a USB drive, a video camera, and a cellular phone. *Id.* at *3. House was questioned by the agents, during which time he informed them that the computer was password protected and refused to disclose the password because it would allow unauthorized access to his employer's server. *Id.* When House was allowed to leave, his phone was returned to him but the other items were not. *Id.* at *4. Forty-eight days later, when the electronic devices still had not been returned, House's attorney sent a letter to DHS, CBP, and ICE requesting the return of House's electronics, as well as information on the chain of custody of any copies made of the information in his electronic devices. *Id.* The next day, the devices were returned, but no information was given as to what information, if any, was copied and what was done with any such copies. *Id.* After his devices were returned to him, House filed suit seeking declaratory and injunctive relief, alleging violations of his First and Fourth Amendment rights. *Id.*

13 In June 2010, House and others organized political support for the defense of Bradley Manning, a United States serviceman deployed in Iraq who was arrested in May 2010 on suspicion of having disclosed restricted material to WikiLeaks....

> The Bradley Manning Support Network [ ], formed by House and others, is an unincorporated association of individuals and organizations. The Support Network is an "international grassroots effort to help accused whistle blower Pfc. Bradley Manning."

House, 2012 WL 1038816, at *2 (internal citations omitted).

Relying on *United States v. Braks,* 842 F.2d 509, 512–13 (1st Cir.1988), the district court found that the search of an electronic device lacked the physical contact and force that made searches of the person so invasive and harmful to dignitary interests. *House,* 2012 WL 1038816, at *6–7. Accordingly, the court held that "the search of House's laptop and electronic devices is more akin to the search of a suitcase and other closed containers holding personal information travelers carry with them when they cross the border which may be routinely inspected by customs and require no particularized suspicion." *Id.* at *7.

Crucial to the court's reasoning was the notion that "[i]t is the level of intrusiveness of the search that determines whether the search is routine, not the nature of the device or container to be searched." *Id.* at *8. Thus the district court declined to recognize an exception to the border search doctrine that would give greater protection to electronically stored information than it would to information carried in other formats. *Id.* But the *House* court relied heavily on *Arnold* and *Ickes* and did not address whether forensic searches inherently may be more intrusive than other types of searches of an electronic device. *Id.* at *7. In any event, the district court found that the chance that House was targeted because of his political views created a sufficient possibility that the motivation underlying the search was unreasonable even if the search itself was not impermissible. *Id.* at *8. The court also found that there are some limits on how long the government may detain property, even if it legitimately was seized. *See id.* at *9. The possibility that a forty-nine-day detention was not reasonably related to the reasons for detaining the electronic devices also was sufficiently strong to defeat a motion to dismiss. *Id.* at *9–10.

***560** There are other cases dealing with computer searches, but none directly resolves the question before me. In *United States v. McAuley,* 563 F.Supp.2d 672 (W.D.Tex.2008), the Western District of Texas held that the conventional search of a "personal computer at a port of entry is a routine search and thus, does not necessitate a finding of reasonable suspicion in order to search a computer, disks, hard drives, or any other technical devices." *Id.* at 679. The court's holding rested on its refusal to create a special rule for computers, because "[a] search of items like a computer, unlike a strip search of a person, is not per se embarrassing," particularly where, as in McAuley's case, that search was done in a private location where others would not see

that he possessed pornographic material. *Id.* at 678–79. The court also found that the existence of a password on the computer was no more relevant than the existence of a lock on a suitcase, neither of which automatically can convert a search from routine to nonroutine. *Id.* at 678. And in *United States v. Romm,* the Ninth Circuit upheld a forensic search of a laptop computer at the border without probable cause, 455 F.3d 990, 1006 (9th Cir.2006), but the only issue raised on that appeal was whether the search in question was a border search; the defendant had waived any argument that the forensic search exceeded the valid scope of a border search. *Id.* at 996–97.

Counsel also have cited several cases in which courts upheld searches of computers or other media as supported by reasonable suspicion, thereby obviating the need to determine whether the search was routine or nonroutine. *See, e.g., United States v. Irving,* 452 F.3d 110, 124 (2d Cir.2006) (upholding border search of floppy disks and undeveloped film without analyzing what type of search had occurred because officers had reasonable suspicion); *United States v. Roberts,* 274 F.3d 1007, 1012 (5th Cir.2001) (assuming that search of diskettes was nonroutine and finding it was supported by reasonable suspicion); *United States v. Furukawa,* No. 06–145(DSD/AJB), 2006 WL 3330726, at *1–2 (D.Minn. Nov. 16, 2006) (finding that search of computer was supported by reasonable suspicion and therefore it did not matter whether it was routine or nonroutine).

D. An Analytical Framework for Searches of Electronic Media

[18] "There is no question that computers are capable of storing immense amounts of information and often contain a great deal of private information. Searches of computers therefore often involve a degree of intrusiveness much greater in quantity, if not different in kind, from searches of other containers." *United States v. Payton,* 573 F.3d 859, 862–63 (9th Cir.2009). But the Fourth Circuit has stated that a conventional search of a computer is not legally distinct from a conventional search of a closed container. *See Ickes,* 393 F.3d at 503, 507; *see also Arnold,* 533 F.3d at 1010.

A conventional search at the border of a computer or device may include a Customs officer booting it up and operating it to review its contents, and seemingly, also would allow (but is not necessarily limited to) reviewing a computer's directory tree or using its search functions to seek out and view the contents of specific files or file types. Because electronic storage is logical, not spatial or physical, even a cursory search can be tremendously powerful because it can target very specific files or file types. *See* Orin S. Kerr, *Searches and Seizures in a Digital World,* 119 Harv. L.Rev. 531, 540, 544–47 (2005). And, just as a luggage lock does not render the contents of a suitcase immune from search, a password protected file is not unsearchable ***561** on that basis alone. *See McAuley,* 563 F.Supp.2d at 678.

But seizing a digital device, imaging the entirety of its contents, and keeping the imaged file in the possession of the government after the device has been returned for the purpose of subjecting the imaged file to a forensic search, is another matter entirely. In a forensic search of electronic storage, a bitstream copy is created and then is searched by an expert using highly specialized analytical software—often over the course of several days, weeks, or months—to locate specific files or file types, recover hidden, deleted, or encrypted data, and analyze the structure of files and of a drive. *See* Kerr, *supra,* at 544–47. It is the potentially limitless duration and scope of a forensic search of the imaged contents of a digital device that distinguishes it from a conventional computer search. The latter may take hours and delve deeply into the contents of the device, but it is difficult to conceive of a conventional search of a computer or similar device at a border lasting days or weeks. A forensic examination of the imaged content, possibly at a location far from the border and using sophisticated electronic search methods designed to recover even deleted information, is of an altogether different scope and magnitude. And while courts may reach different conclusions about whether forensic searches of digital devices seized at the border require reasonable suspicion, they nevertheless should acknowledge the true character of the devices at issue, the amount of data they contain, the mix of personal and business information they store, and the magnitude of what their contents may reveal about the lives of their users. Facile analogies of forensic examination of a computer or smartphone to the search of a briefcase, suitcase, or trunk are no more helpful than analogizing a glass of water to an Olympic swimming pool because both involve water located in a physical container. "Judges and lawyers live on the slippery slope of analogies; they are not supposed to ski it to the bottom." Robert H. Bork, *The*

Tempting of America: The Political Seduction of the Law 169 (1990).

The courts that have confronted forensic searches have struggled to differentiate between general characteristics of searches of electronic devices and characteristics unique to forensic searches as such. *See supra* (explaining that neither *Cotterman* nor *Abidor* drew a clear distinction between a forensic search and a conventional one). This distinction seems absolutely necessary for analyzing the constitutional requirements for forensic searches.

1. Issues Raised by Electronic Devices Generally

The proliferation of electronic devices has allowed travelers to carry a tremendous amount of information with them, much of which is likely to be highly personal. The sheer quantity of data strains analogies between computers and other closed containers. For example, the standard size of a checked bag on an international flight is sixty-two linear inches (that is, the total of length plus width plus height) and fifty pounds. *See, e.g., American Airlines Baggage Allowance Information,* American Airlines, http://www.aa.com/i 18n/travelInformation/baggage/ baggageAllowance.jsp# ! basic-info/ (last visited Apr. 4, 2014) (checked bags may be up to 62 linear inches and fifty pounds); *Checked Bags & Fees,* Delta, http://www.delta.com/content/www/en_US/traveling-with-us/baggage/before-your-trip/checked.html?icid=Policy_Ck_Baggage_Ongoing/ (last visited Apr. 4, 2014) (same); *Baggage Policies,* U.S. Airways, http:// www.usairways.com/enUS/traveltools/baggage/baggagepolicies.html (last visited Apr. 4, ***562** 2014) (same); *see also Checked Baggage,* United, http://www. united.com/CMS/en-US/travel/Pages/BaggageChecked.aspx (last visited Apr. 4, 2014) (checked bags may be up to 62 linear inches and fifty pounds or up to seventy pounds for certain passengers). In contrast, LexisNexis estimates that a single gigabyte of data can comprise nearly sixty-five thousand pages of Microsoft Word documents, over one hundred thousand pages of e-mails, or nearly six hundred seventy-eight thousand pages of text files. LexisNexis, How Many Pages in a Gigabyte, http://www.lexisnexis.com/applied discovery/lawlibrary/whitepapers/adi_fs_pagesinagigabyte.pdf (last visited Apr. 4, 2013). If one gigabyte of Word documents was printed on standard, 8.5#x11#, twenty pound paper, the paper would occupy enough space to fill at least four suitcases (each measuring 30# x 20# x 12#—that is, sixty-two linear inches) and would weigh 650 pounds, which would require thirteen checked bags. [14] Using this math, the eight-gigabyte USB drive that Saboonchi was carrying could hold the equivalent of thirty-two suitcases based on its size and, at 5,200 pounds, would exceed the weight limit for one hundred checked suitcases. [15]

14 One ream of twenty pound paper weighs five pounds and contains five hundred pages; one case of paper contains ten reams and, according to Amazon.com, has the approximate dimensions of 17.6# x 115# x 10.8#. *Xerox 4200 Business Multipurpose White Paper, 92 Bright, 8–1/2 x 11, 10 Reams/Carton (XER3R2047),* Amazon.com, http://www.amazon.com/Xerox-Business Multipurpose-Bright-XER3R2047/dp/B000093IO4/ref=sr_1_7?ie=UTF 8&qid=1392922161&sr=8–7 (last visited Apr. 4, 2014).

15 The USB drive likely is only the tip of the iceberg. The iPhone 4s that Saboonchi was carrying, *see* ICE Report 1, is available with a storage capacity ranging from eight to sixty-four gigabytes. *Identifying iPhone Models,* Apple.com, http://support.apple.com/kb/ht3939 (scroll to iPhone 4s) (last visited Apr. 4, 2014). The Sony Ericsson Xperia phone that Saboonchi was carrying contained a microSD card with a sixteen gigabyte capacity. *See* Ice Report 1. A microSD card provides removable storage for up to 128 gigabytes, *see, e.g., Sandisk microSD Cards,* SanDisk, http://www.sandisk.com/products/memory-cards/microsd/ (last visited Apr. 4, 2014), and is about the size of a thumbnail, *see, e.g., SanDisk Ultra 128 GB microSDXC UHS–I Card with Adapter (SDSDQUA 128G–G46A),* Amazon.com, http://www.amazon.com/SanDisk–Ultra–microSDXC–Adapter–SDSDQUA–128G–G46 A/dp/B00IIJ6W4S/ref=sr_1_28?sic&ie=UTF8&qid=1393515338&sr=1–28&keywords=micro+sd+128gb (listing the dimensions of a microSD card as 0.6# x 0.4#) (last visited Apr. 4, All of this pales in comparison to laptop computers currently being sold with a hard drive capacity of up to one terabyte (1,024 gigabytes). *See, e.g., Compare Mac Models,* Apple.com, http://www.apple.com/mac/compare/ notebooks.html (listing standard hard

> drive size for a MacBook Pro as up to one terabyte) (last visited Apr. 4, 2014).

There also is no question that a conventional search allows Customs officers to examine a wealth of information that

> is, by and large, of a highly personal nature: photographs, videos, written and audio messages (text, email, and voicemail), contacts, calendar appointments, web search and browsing history, purchases, and financial and medical records. It is the kind of information one previously would have stored in one's home that would have been off limits to officers performing [a border search].

United States v. Wurie, 728 F.3d 1, 8 (1st Cir.2013), *cert. granted,* —— U.S. ——, 134 S.Ct. 999, 187 L.Ed.2d 848 (2014) (internal citations omitted). But this type of search has been indispensable in allowing Customs officers to uncover concealed child pornography, *see, e.g., Arnold,* 533 F.3d at 1005; pictures of terrorist groups, *see Abidor,* 990 F.Supp.2d at 267–68, 2013 WL 6912654, at *5; and evidence of drug activities, ***563** *see United States v. Rodridiguez,* No. C–11–344, 2011 WL 3924958, at *2 (S.D.Tex. Sept. 6, 2011) (CBP agents found pictures of marijuana on a cell phone), even when they were protected by a password, *see, e.g., United States v. McAuley,* 563 F.Supp.2d at 674. Officers also have found evidence of criminal activities in conventional searches of text messages, e-mails, internet histories, and call logs. *See, e.g., United States v. Finley,* 477 F.3d 250, 254 (5th Cir.2007) (scrolling through text messages revealed messages related to narcotics use and trafficking); *United States v. Kyle,* No. CR 10–00245–1 JSW, 2011 WL 176038, at *2 (N.D.Cal. Jan. 19, 2011) (officers searched cell phone for e-mails, text messages, and call logs).

But even though travelers routinely walk around carrying digital truckloads worth of data, a conventional search of an electronic device does not differ significantly in scope from the search of a suitcase. There is a limited amount of time that can be devoted to this while the owner waits at the border for the search to conclude and, even if "[t]he private information individuals store on digital devices—their personal 'papers' in the words of the Constitution—stands in stark contrast to the generic and impersonal contents of a gas tank," *Cotterman,* 709 F.3d at 964 (citing *United States v. Jones,* —— U.S. ——, 132 S.Ct. 945, 957, 181 L.Ed.2d 911 (2012) (Sotomayor, J., concurring)), a conventional search of a digital device—though by no means limited to *Abidor's* "quick search"—necessarily must focus on turning up evidence of contraband or illegal activity within a reasonably limited amount of time. The mere fact that this information may be located more readily on a computer does not change the nature of the search. *See United States v. Knotts,* 460 U.S. 276, 285, 103 S.Ct. 1081, 75 L.Ed.2d 55 (1983) (using a beeper to augment visual surveillance of a suspect on public roadways was permissible because "scientific enhancement of this sort raises no constitutional issues which visual surveillance would not also raise").

Nor do the privacy concerns raised by such a search differ from where a traveler brings a suitcase full of personal items, files, or a diary. Although it surely is a discomforting concept, there is no principle beyond the shortness of life and the acknowledgement that there is only so much time available to conduct any particular border search that prevents a CBP officer from "reading a diary line by line looking for mention of criminal activity." *Cf. Cotterman,* 709 F.3d at 962–63. But in practice, CBP officers are expected to use their discretion to focus on more likely evidence of contraband or criminality—to ensure that what appears to be a diary is not actually *The Anarchist Cookbook,* and to move on.

All of this is not to say that there are not new issues on the horizon that may not fit into existing frameworks. Cloud computing allows users to store data on a remote server for easy access from a computer or cell phone, "giv[ing] users 'anywhere access' to applications and data stored on the Internet." David A. Couillard, Note, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing,* 93 Minn. L.Rev. 2205, 2216 (2009). These files do not "cross the border, [but they] may appear as a seamless part of the digital device when presented at the border." *Cotterman,* 709 F.3d at 965. It is not clear how these files should be treated in a border search.

Even more concerning, Judge Posner has noted that "[a]n iPhone application called iCam allows you to access your home computer's webcam so that you can survey the inside of your home while ***564** you're a thousand miles away. At the touch of a button a cell phone search becomes a house search, and that is not a search of a 'container'

in any normal sense of that word, though a house contains data." *United States v. Flores–Lopez,* 670 F.3d 803, 806 (7th Cir.2012) (internal citations omitted). This technology raises the possibility that some conventional searches may run afoul of *Kyllo v. United States,* 533 U.S. 27, 38, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001) (holding that advances in technology cannot "erode the privacy guaranteed by the Fourth Amendment"), but these questions are for another court to consider on another day, and are not before me now.

In sum, the reason why a conventional search of a computer can be analogized to a conventional search of a suitcase is less because a computer is analogous to a suitcase than it is because a conventional search has the same inherent limitations—and the same inherent risk of invasiveness—irrespective of what is being searched. There is only a finite amount of time available for a CBP agent to detain a traveler at the border to search the contents of his suitcase or laptop. If the collected works of Shakespeare comprise a mere five megabytes of text, *see Data Powers of Ten,* in *How Much Information* (2000), http://www2.sims.berkeley.edu/research/projects/how-much-info/datapowers.html, a conventional search of a hard drive containing several gigabytes of data cannot possibly encompass every bit of data on the device to be searched any more than a search of an English major's bags would include a full reading of *Hamlet.* There simply is not enough time to do so while both traveler and Customs agent wait at the border.

2. Issues Unique to Forensic Searches

In contrast, a forensic search is a different *search*—not merely a search of a different object—and it fundamentally alters the playing field for all involved. A forensic search requires the creation of a bitstream copy and its thorough analysis with specialized software over an extended period of time. *See* Kerr, *supra,* at 540, 544–47. This type of search raises issues that do not arise in conventional searches. First, because the item searched is a bitstream copy of a device, it may take place long after the device itself has been returned to its owner and therefore a forensic search is unbounded in time. Second, a forensic search allows officers to recover a wealth of information even after it has been deleted. And third, a forensic search provides information about a person's domestic activities away from the border that is not otherwise available even in a conventional search taking place at the border.

i. The Role of Imaging Software

The subject of a forensic search always is a bitstream copy of the data on a device—and copies of the copy—not the device itself. *See* Kerr, *supra,* at 540 ("The actual search occurs on the government's computer, not the defendant's."); *see also* ICE Report 1 (noting that each device was "connected to an XRY imaging machine and a logical image ... was obtained," following which the "device was then returned to evidence storage"). The primary purpose of working from an image is to "duplicate[ ] every bit and byte on the target drive including all files, the slack space, Master File Table, and metadata in exactly the order they appear on the original." Kerr, *supra,* at 541. It also prevents the alteration or loss of data as a result of the operation of a computer itself. *Cf.* Corey J. Mantei, Note, *Pornography and Privacy in Plain View: Applying the Plain View Doctrine to Computer Searches,* 53 Ariz. L.Rev. 985, 1007 (2011) ("[A] manual search of an operating system may lead to evidentiary issues because ***565** of compromised or damaged hardware, data loss, or poor forensic analysis.").

But creating an image of a drive has an added benefit to law enforcement: "Instead of detaining the electronic device, CBP or ICE may instead copy the contents of the electronic device for a more in-depth border search at a later time." U.S. Dep't of Homeland Sec., *Privacy Impact Assessment for the Border Searches of Electronic Devices* 8 (Aug. 25, 2009), http://www.dhs. gov/xlibrary/assets/privacy/privacy_pia_cbp_laptop.pdf [hereinafter Privacy Impact Assessment]. This allows for searches to extend far beyond the time that an actual physical search at the border would have been performed. Whereas the sixteen hour detention of Montoya de Hernandez "undoubtedly exceed [ed] any other detention ... approved under reasonable suspicion," *Montoya de Hernandez,* 473 U.S. at 543, 105 S.Ct. 3304, "[c]omputer searches tend to require fewer people but more time," Kerr, *supra,* at 544, and the forensic review of imaged files routinely lasts days if not weeks, *see, e.g., United States v. Mutschelknaus,* 592 F.3d 826, 828 (8th Cir.2010) (search warrant provided for search of home within ten days, but allowed an additional sixty days for the forensic review of computers). Indeed, the Federal Rules of Criminal Procedure acknowledge this

by expressly providing that the fourteen-day time limit to execute a warrant applies only to "the seizure or on-site copying of the media or information, and not to any later off-site copying or review." Fed.R.Crim.P. 41(e)(2)(B). To the extent that the ability exists to execute a search long after a physical device has been returned to its owner, this allows Customs officers to search a computer days or even weeks after it physically has entered the country. In such circumstances, it no longer can be said that the purpose of the search is to prevent contraband from entering the country, and the search has become uncoupled from the rationale for its justification. *See Flores–Montano,* 541 U.S. at 153, 124 S.Ct. 1582. Also, forensic "[c]omputer searches lower the cost and inconvenience of invasive searches, making such searches the norm rather than the exception." Kerr, *supra,* at 569–70. If unchecked by even the need to show something as minimal as articulable suspicion, a forensic search of a hard drive containing vast amounts of digital information, unbounded by limits of time, space, or human stamina, bears little resemblance to the type of search that historically has been justified in the name of securing the borders of the country.

And "even if the initial seizure of a laptop and other electronic devices at the border requires no reasonable suspicion, the '[g]overnment cannot simply seize property under its border search power and hold it for weeks, months, or years on a whim.' " *House v. Napolitano,* No. 11–10852–DJC, 2012 WL 1038816, at *9 (D.Mass. March 28, 2012) (quoting *U.S. v. Cotterman,* 637 F.3d 1068, 1070, 1082–83 (9th Cir.2011) (alteration in original)). Even when acting under the border search doctrine, a particularly lengthy seizure raises concerns where "the detention [is not] reasonably related in scope to the circumstances which justified it initially." *Montoya de Hernandez,* 473 U.S. at 542, 105 S.Ct. 3304. Assuming, without deciding, that the creation and retention of a bitstream copy implicates at least some of the same concerns as a traditional seizure of physical evidence, [16] there is a fundamental difference between allowing a Customs ***566** officer to review a computer as it crosses the border and allowing CBP, HSI, and related agencies to use a border crossing as a license to obtain a full copy of any electronic device to be perused at a later date.

16 It is not entirely clear whether retaining an image of electronic data constitutes a "seizure." In the physical world, it has been established that so long as an action does not " 'meaningfully interfere' with [the owner's] possessory interest," a seizure has not occurred even if information related to an item is recorded. *See Arizona v. Hicks,* 480 U.S. 321, 324, 107 S.Ct. 1149, 94 L.Ed.2d 347 (1987). But electronic information is "nonrivalrous. It simply cannot be 'used up.' Indeed, copying information actually multiplies the available resources," so that both the original owner and the copier may have equally good copies of the same data. Mark A. Lemley, *Ex Ante Versus Ex Post Justifications for Intellectual Property,* 71 U. Chi. L.Rev. 129, 143 (2004). At the very least, it has been suggested that generating a bitstream copy at least could be considered "a search or seizure based on its interference with the owner's property rights." *See, e.g.,* Kerr, *supra,* at 535.

ii. Access to Deleted Data

A forensic search also exposes an entirely different body of data from any conventional search: It is the only means by which deleted data can be recovered. [17] *See* Kerr, *supra,* at 542–43. Indeed, one of the specific purposes of the forensic search in this case was to "allow[ ] the unallocated sectors of the disk to be searched and examined" to recover deleted files. ICE Reports 2. As Kerr explained:

17 And unlike when physical trash is discarded, information deleted from an electronic device is not otherwise exposed to the public. *Cf. California v. Greenwood,* 486 U.S. 35, 40, 108 S.Ct. 1625, 100 L.Ed.2d 30 (1988).

> [M]arking a file as "deleted" normally does not actually delete the file; operating systems do not "zero out" the zeroes and ones associated with that file when it is marked for deletion. Rather, most operating systems merely go to the Master File Table and mark that particular file's clusters available for future use by other files. If the operating system does not reuse that cluster for another file by the time the computer is analyzed, the file marked for deletion will remain undisturbed. Even if another file is assigned to that cluster, a tremendous amount of data often can be recovered from the hard drive's "slack space," space within a cluster left temporarily unused. It can be accessed by an analyst just like any other file.
>
> Computer operating systems and programs also generate and store a wealth of information about how the computer and its contents have been

> used. As more programs are used, that information, called metadata, becomes broader and more comprehensive. For example, the popular Windows operating system generates a great deal of important metadata about exactly how and when a computer has been used. Common word processing programs such as WordPerfect and Microsoft Word generate temporary files that permit analysts to reconstruct the development of a file. Word processing documents can also store data about who created the file, as well as the history of the file. Similarly, browsers used to surf the World Wide Web can store a great deal of detailed information about the user's interests, habits, identity, and online whereabouts, often unbeknownst to the user. Browsers typically are programmed to automatically retain information about the websites users have visited in recent weeks; users may use this history to retrace their steps or find webpages they previously visited. Some of this information may be very specific; for example, the address produced by an Internet search engine query generally includes the actual search terms the user entered.

Id. at 542–43 (footnotes omitted).

Indeed, even reformatting a hard drive—which long has been described as ***567** the only truly final way to delete sensitive information from a drive—often "erases less than 1/10th of one percent of the data on the disk, such that anyone with rudimentary computer forensic skills can recover your private, privileged and confidential data. If it's not overwritten or physically destroyed, it's not gone." Craig Ball, *Computer Forensics for Lawyers Who Can't Set a Digital Clock* 3, 25, *in Five on Forensics* (2008), http://www. craigball.com/_OFFLINE/cf.pdf. This means that *Abidor's* injunction that users should " '[t]hink twice about the information [they] carry on [their] laptop,' " *Abidor,* 990 F.Supp.2d at 277, 2013 WL 6912654, at *14 (quoting *Airport Insecurity: The Case of the Lost & Missing Laptops,* Ponemon Institute LLC, 3 (July 29, 2008), http://www.dell.com/ downloads/global/services/ dell_ lost_laptop_study_emea.pdf), misses the point. No matter how many times a user tries to protect herself by removing private or extraneous data from her computer, her efforts will be fruitless in the event of a forensic search capable of uncovering anything that may have been on the computer at any point in time. And these files can remain in a computer's slack space for "months, even years," Philip N. Yannella, *How the Latest Advances in Computer Forensic Analysis Are Impacting Litigation Matters,* Aspatore, Aug. 2013, 2013 WL 3759816, at *1, meaning that a user who wishes to be protected against forensic border searches would be well advised *never* to put private or personal data on her computer or smartphone; by the time a foreign trip is on the horizon it will be far too late to delete any such data. [18]

18 Though there are tools, such as Apple's "Secure Empty Trash" feature, *see OS X Mountain Lion: Prevent Deleted Files from Being Read,* Apple.com, http://support.apple.com/kb/PH11124 (last visited Apr. 4, 2014), that may enable a user permanently to erase data from a computer, these are special features or applications that a typical user may not even be aware of, and their existence does not affect the reality that the overwhelming majority of users of electronic devices operate under the reasonable belief that once they have deleted an item permanently, it is gone.

And even if a user *never* saves any data, there still is no guarantee of protection because a forensic search can recover even some unsaved data. This goes beyond a mere search of one's "papers" to a review of their thoughts and ideas left unspoken. [19] It may include deeply personal thoughts that no sooner were typed than deleted, months—or years-old internet search history and communications, and pictures or documents long-since discarded. Rather than a search of a suitcase, this would be as if, by opening a suitcase, a Customs officer could determine everywhere the suitcase had been taken, everything that had been packed within it, when and how it was acquired, and when each item last had been worn. The prospect stretches the computer-to-closed-container analogy beyond its breaking point.

19 This problem was even more prevalent under older file systems, in which unfilled clusters would be "padded" with whatever happened to be in the computer's Random Access Memory at that moment —which would include whatever the user had done recently irrespective of whether it ever was saved to disk. *See* Ball, *supra,* at 27.

iii. Access to Protected Information

A forensic search of a mobile device also can reveal a wealth of data about a user's day-to-day life. "Security researchers have discovered that Apple's iPhone keeps track of where you go—and saves every detail of it to a secret file on the device," including latitude and longitude data and timestamps, for up to a year. Charles

Arthur, *iPhone Keeps Record of Everywhere You Go,* The Guardian (U.K.) (Apr. ***568** 20, 2011 9:06 AM), http://www.theguardian. com/technology/2011/apr/20/iphone-tracking-prompts-privacyfears. Devices using the Android operating system also store similar data, gleaned from cell tower triangulation and from WiFi networks that they encounter. Chris Foresman, *Android Phones Keep Location Cache, Too, But It's Harder to Access,* Ars Technica (Apr. 22, 2011 2:37 PM), http://arstechnica. com/gadgets/2011/04/android-phones-keep-location-cachetoo-but-its-harder-to-access/. In Saboonchi's case, the search also recovered WiFi connection information, ICE Reports 2, that can be used to determine a user's location, *see* Foresman, *supra.* That means that a Customs officer performing a forensic search can recreate the most intimate details of a person's life over the course of the last several months—even if the data includes highly personal details of what transpired before leaving the country or while in one's own home. *See In re Application of United States,* 849 F.Supp.2d 526, 540 (D.Md.2011) ("Location data from a cell phone is distinguishable from traditional physical surveillance because it enables law enforcement to locate a person entirely divorced from all visual observation."). "Indiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight." *United States v. Karo,* 468 U.S. 705, 716, 104 S.Ct. 3296, 82 L.Ed.2d 530 (1984).

And this is to say nothing about the reams of data that, though readily available on a smartphone or computer, nevertheless are unlikely to be reviewed and analyzed at length in a conventional search. The forensic searches of Saboonchi's Devices recovered contacts, call logs, calendar entries, text messages, email, chat logs, web browser information, photos, documents, and video files. ICE Reports 2; *see also supra* (explaining that forensic searches essentially are unbounded in time).

iv. A Forensic Search Is Sui Generis

Taking all of this into account, I cannot help but find that even if a computer or cell phone is analogized to a closed container, a forensic search cannot be analogized to a conventional search of luggage or even of a person. A forensic search is far more invasive than any other property search that I have come across and, although it lacks the discomfort or embarrassment that accompanies a body-cavity search, it has the potential to be even more revealing.

A conventional computer search allows Customs officers to choose, within the finite amount of time available to them while they detain the traveler, to decide where, within a veritable mountain of personal data, to focus their attention while searching for contraband, threats, or criminality. And at the end of a conventional search, as with the conventional search of a suitcase, a traveler regains custody of his possessions and information and proceeds about his business with a minimum of lingering inconvenience. A forensic search, on the other hand, allows a Customs officer to give uniquely probing review not only to the files on one's computer, but also any files that ever may have been on that computer. And even after a traveler is cleared to enter the country, the search may continue for months or even years afterwards.

Applying the *Braks* factors, there is no doubt that such a search results in the exposure of intimate details and abrogates a traveler's reasonable expectations of privacy in his or her most personal and confidential affairs—including in information that, from the user's perspective, no longer even exists. *United States v. Braks,* 842, ***569** F.2d 509, 512 (1st Cir.1988). And although such a search may not always involve physical contact or force, *id.,* a Customs officer at least must make contact with a device to operate it, and it is not unheard of for officers to apply some measure of additional force to the item searched, *see Abidor,* 990 F.Supp.2d at 268, 2013 WL 6912654, at *5 (noting that it looked like the plaintiff's devices "had been physically opened"), and in any event it frequently deprives the person whose devices are searched of his or her possessions for several days, if not weeks, *see, e.g.,* Def.'s Mot. 3, 6 (noting that the Devices were confiscated on March 31, 2012 and returned to Defendant two weeks later on April 13, 2012); *Abidor,* 990 F.Supp.2d at 268, 2013 WL 6912654, at *5 ("Abidor's laptop and external drive were returned to him eleven days later by mail."); *House,* 2012 WL 1038816, at *4 (plaintiff's devices were in government custody for forty-nine days).

My conclusion becomes even more clear if I focus on the potential for personal indignity and intrusiveness—as did the Eleventh Circuit in *Vega–Barvo*—because a computer forensic search is at least as invasive as an x-ray,

takes longer, and reveals considerably more information. *See United States v. Vega–Barvo,* 729 F.2d 1341, 1345 (11th Cir.1984). And, particularly because it may contain location data, a forensic search of a mobile device also may reveal information about what goes on within the privacy of one's home, which even at the border is subject to heightened protection. *See United States v. Whitted,* 541 F.3d 480, 488 (3d Cir.2008).

It is true that there are not many existing cases in which property searches were found to be nonroutine, but the Supreme Court has not foreclosed the possibility that such a category of search may exist. *See Flores–Montano,* 541 U.S. at 154 n. 2, 124 S.Ct. 1582. It is difficult to conceive of a property search more invasive or intrusive than a forensic computer search—it essentially is a body cavity search of a computer. If any property search can be considered nonroutine, a forensic search of an electronic device must fall into that category. Its ability to plumb the depths of a traveler's data differs not only in degree, but in kind, from conventional searches. Accordingly, under the facts presented to me in this case, I find that a search of imaged hard drives of digital devices taken from the Defendant at the border and subjected to forensic examination days or weeks later cannot be performed in the absence of reasonable suspicion.

v. The Scope of this Ruling

I also must clarify what I do not hold today. First, nothing in this opinion departs from the Fourth Circuit's holding in *Ickes.* It would be unworkable to develop a different set of rules for conventional border searches of computers, not to mention for anything capable of containing expressive material. *See Ickes,* 393 F.3d at 506.

I also do not define a forensic search in terms of the amount of data that is recovered, thereby leaving the status of a given search to be resolved later by Customs officers. *Cf. Cotterman,* 709 F.3d at 967. A forensic search is a different procedure, fundamentally, from a conventional search. It occurs when a computer expert creates a bitstream copy and it analyzes it by means of specialized software. Because the distinction between a conventional computer search at the border that requires no showing of suspicion and a forensic examination of the imaged hard drive of a computer or digital device is easy to distinguish, the narrow holding of this decision does not hamper the ability of Customs officers to perform their duties when ***570** conventionally searching digital devices at the border.

Moreover, as explained, forensic searches are not prohibited—or even subject to a difficult or exacting level of constitutional scrutiny. All that is required is that a Customs officer has reasonable suspicion—that is, a " 'particularized and objective basis for suspecting the particular' " device to be searched contains contraband or evidence of criminal activity. *See Montoya de Hernandez,* 473 U.S. at 541–42, 105 S.Ct. 3304 (quoting *United States v. Cortez,* 449 U.S. 411, 417, 101 S.Ct. 690, 66 L.Ed.2d 621 (1981)). This standard is far from onerous and still leaves officers with considerable freedom to search suspicious persons and respond to unexpected factual developments. *See, e.g., United States v. Brignoni–Ponce,* 422 U.S. 873, 884–85, 95 S.Ct. 2574, 45 L.Ed.2d 607 (1975) ("Any number of factors may be taken into account in deciding whether there is reasonable suspicion to stop a car in the border area.... In all situations the officer is entitled to assess the facts in light of his experience in detecting illegal entry and smuggling." (citations omitted)).

Nor is my ruling likely meaningfully to change anything that actually happens at the border. The Department of Homeland Security has advised CBP officers that "[i]n the course of a border search, with or without individualized suspicion, an Officer may examine electronic devices and may review and analyze the information encountered at the border." CBP Directive § 5.1.2, Privacy Impact Assessment Attachment 1. This has not changed. CBP Officers also might detain an electronic device "to perform a thorough border search." CBP Directive § 5.3.1. So long as that search is conventional, and not forensic—and so long as the time for which the device is detained is reasonably related in scope to the circumstances requiring the search, *see House,* 2012 WL 1038816, at *9—this also remains permissible. Insofar as CBP only will retain information beyond the length of the initial search with probable cause, CBP Directive § 5.4.1.1, that requirement goes beyond anything required by this opinion. And although there is some lack of clarity as to precisely when and how DHS allows data to be analyzed, it has noted that data typically will be retained—that is, "store[d] ... in any of their recordkeeping systems"—if "the border search reveals information relevant to immigration, customs, or other laws enforced by DHS." Privacy Impact Assessment

5. Again, this remains permitted because it presupposes a reasonable suspicion.

Finally, I am not aware of a single case that would have reached a different outcome on the basis of the reasoning in my ruling here. Put simply, Customs officials do not have the time or resources—or, most likely, the inclination—to perform random or suspicionless forensic searches. *See, e.g., United States v. Chaudhry,* 424 F.3d 1051, 1054 (9th Cir.2005) (Fletcher, J., specially concurring) ("As a practical matter, border agents are too busy to do extensive searches (removing gas tanks and door panels, boring holes in truck beds) unless they have suspicion."); *Abidor,* 990 F.Supp.2d at 282, 2013 WL 6912654, at *18 ("I would agree with the Ninth Circuit that, if suspicionless forensic searches at the border threaten to become the norm, then some threshold showing of reasonable suspicion should be required."). Indeed, neither I nor the parties have found any case where a forensic search was performed in the absence of reasonable suspicion, *see Cotterman,* 709 F.3d at 970; *United States v. Stewart,* 729 F.3d 517, 520 (6th Cir.2013); *Abidor,* 990 F.Supp.2d at 282–83, 2013 WL 6912654, at *18–19; *see also* ***571** *United States v. Irving,* 452 F.3d 110, 124 (2d Cir.2006); *United States v. Roberts,* 274 F.3d 1007, 1012 (5th Cir.2001); *United States v. Furukawa,* No. 06–145(DSD/AJB), 2006 WL 3330726, at *1–2 (D.Minn. Nov. 16, 2006).

E. The Search of Saboonchi's Devices Was Supported by Reasonable Suspicion

[19] When Saboonchi arrived at the Rainbow Bridge on March 31, 2012, he already was the subject of an investigation. His name had come up in connection with two different investigations of export violations. Baird Tr. 10:21–11:23. Several subpoenas seeking evidence about Saboonchi's dealings already had been issued and were returned in early March 2012. *Id.* at 11:24–12:2. The information that was received in response to those subpoenas showed that Saboonchi had purchased two cyclone separators after representing that they would be used domestically, *id.* at 12:13–22, and then shipped them overseas, *id.* at 12:2–7, understating the value of the cyclone separators in a manner consistent with an attempt to avoid scrutiny, *id.* at 16:6–8. Special Agent Baird also had determined that the recipient of the cyclone separators, General DSAZ, was linked to an industrial parts company in Iran. *Id.* at 12:8–12.

All of this is more than sufficient to give rise to reasonable, particularized suspicion—if not probable cause—that Saboonchi was involved in violations of export restrictions on Iran. Accordingly, CBP and HSI officers did not violate the Fourth Amendment when they seized Saboonchi's Devices and subjected them to a forensic search.

IV. CONCLUSION

In sum, for the reasons stated above, Defendant's Motion to Suppress, ECF No. 58, is DENIED, as was ordered on the record in open Court.

All Citations

990 F.Supp.2d 536

End of Document