No.____

In The Supreme Court of The United States

Daren W. Phillips,

Petitioner,

v.

United States of America,

Respondent.

On Petition for a Writ of Certiorari to the
United States Court of Appeals for the Ninth Circuit

Petitioner's Appendix

FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, *Plaintiff-Appellee*, v. DAREN W. PHILLIPS, *Defendant-Appellant.*	No. 20-10304 D.C. No. 3:18-cr-00101- MMD-WGC-1 OPINION

Appeal from the United States District Court
for the District of Nevada
Miranda M. Du, Chief District Judge, Presiding

Argued and Submitted November 15, 2021
San Francisco, California

Filed April 29, 2022

Before: Richard A. Paez and Michelle T. Friedland, Circuit Judges, and Edward R. Korman,* District Judge.

Opinion by Judge Korman

* The Honorable Edward R. Korman, United States District Judge for the Eastern District of New York, sitting by designation.

SUMMARY[**]

Criminal Law

The panel affirmed a judgment of conviction in a case in which Daren Phillips entered a conditional guilty plea to possession of child pornography, reserving the right to appeal the denial of his motion to suppress evidence found on his laptop computer.

After calling off her engagement to Phillips, Amanda Windes discovered child pornography on his computer, which she then brought to the Washoe County Sheriff's Office. While Windes was there, Detective Gregory Sawyer asked her to show him only images that she had already viewed when she had accessed the laptop by herself. Windes complied with that request.

Phillips moved to suppress on the ground that, because Sawyer directed Windes to access the computer without Phillips's permission to show Sawyer what she had already seen, Windes's search of the computer at the sheriff's office was an unlawful law-enforcement search.

Because the U.S. Attorney does not dispute Phillips's assertion that Windes acted as a state agent when she accessed the computer at the sheriff's office, the panel assumed that this was a government search.

But applying *United States v. Jacobsen*, 466 U.S. 109 (1984), and *United States v. Bowman*, 215 F.3d 951 (9th Cir.

[**] This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

2000), the panel held that the search was permissible because, as the parties agree, when Windes accessed the child pornography on Phillips's computer at the sheriff's office, she merely mimicked her earlier private search. The panel rejected Phillips's argument that *Jacobsen* imposes requirements tied to law enforcement's subjective knowledge. The panel distinguished *United States v. Young*, 573 F.3d 711 (9th Cir. 2009), on the ground that this case does not involve a warrantless entry into a home or its equivalent. The panel rejected Phillips's argument that the "common-law trespassory test" set forth in *United States v. Jones*, 565 U.S. 400 (2012), requires suppression in this case.

Noting that in light of Phillips's valid appeal waiver he may argue on appeal only that the supervised-release conditions he challenges exceed the permissible statutory penalty or violate the Constitution, the panel wrote that this court's precedents establish the legality of all the challenged conditions (risk notification, prohibiting access to sexually explicit conduct material involving adults, polygraph testing).

COUNSEL

Aarin E. Kevorkian (argued), Assistant Federal Public Defender; Rene L. Valladares, Federal Public Defender; Office of the Federal Public Defender, Las Vegas, Nevada; for Defendant-Appellant.

William R. Reed (argued), Assistant United States Attorney; Elizabeth O. White, Appellate Chief; Christopher Chiou, Acting United States Attorney; United States Attorney's Office, Reno, Nevada; for Plaintiff-Appellee.

OPINION

KORMAN, District Judge:

In early 2018, Amanda Windes decided to call off her engagement to Daren Phillips. She believed Phillips had been lying to her about his alcohol use and financial troubles. She had also found "very inappropriate" text messages between Phillips and other women. Windes informed Phillips that he was no longer welcome in the house they shared. Two days later Phillips acknowledged that he needed help for his alcoholism, and Windes drove Phillips to a hospital, which arranged for a one-month stay at a residential treatment center. Windes had custody of many of Phillips's possessions while he was away, including his laptop computer. Windes was contacted by Phillips's ex-wife, Kelly Greek, who was worried about how Phillips would pay child support while he was in treatment. Greek also told Windes that she suspected that Phillips had watched child pornography and that Phillips may have been sexually interested in a friend of Greek's daughter.

Windes decided to examine Phillips's laptop. She said that her primary purpose was to examine his financial documents but that she also wanted to see if Phillips had been contacting other women and whether he had been viewing child pornography. She explained that she was also trying "to determine what other issues there w[ere] on top of [Phillips's] alcohol problem for the safety of my children and myself." The laptop was password protected, and Windes first tried the password for Phillips's Netflix account, which he had given to her. That password didn't work, so Windes clicked on the laptop's "forgot your password" function, which prompted her to answer Phillips's security questions. She successfully guessed the answers to those questions, which allowed her to send a

temporary password to her own email account. She was then able to reset the password and enter Phillips's computer.

As Windes browsed Phillips's computer, she came across a folder entitled "phone." She saw that it was several hundred megabytes in size and opened the folder. The folder displayed the names of all the files in the folder and their associated "thumbnail illustration[s]" (a small photo which indicated what each file contained). There were thousands of such thumbnail illustrations in the folder. They included "pictures of infants and all of their exposed genitalia" and "images of young females" who were "very scantily clad and [were in] extremely sexually provocative poses." As she scrolled down through the folder, she saw that many of the file names indicated how old the children were (from infants to teenagers). Windes saw that this "phone" folder contained *only* child pornography. She testified that the images were "highly graphic" and left her "disgusted." She "felt law enforcement needed to further investigate."

Windes first took the laptop to Police Services at the University of Nevada (where she worked) and told them only that she had a computer that she needed somebody to look at. Police Services told her to take the computer to the Washoe County Sheriff's Office ("sheriff's office") because it did not belong to the university. At the sheriff's office, Windes told the front desk deputy that she had a computer that she suspected contained a significant amount of child pornography. She was then interviewed by Detective Arick Dickson for about two-and-a-half hours. Windes told Dickson what she had found and how she had accessed the computer. She described in detail many of the thumbnail images of child pornography she had seen. She also relayed to Dickson her "concerns for . . . [her] children's safety,

especially due to the nature of the material on Phillips'[s] laptop."

Dickson then brought in Detective Gregory Sawyer, who asked Windes to show him only images that she had already viewed when she had accessed the laptop by herself. Windes and Sawyer testified—and the district court found—that Windes complied with that request and showed the detectives only the thumbnail images and accompanying file names she had previously seen while scrolling through the "phone" folder. Only Windes operated the computer while she showed Sawyer the images. Sawyer recognized some of the thumbnail images from prior child pornography investigations. Sawyer then seized the laptop and applied for and obtained a search warrant. The application included a brief written description of two thumbnail images that Windes had shown him and the associated file names. A subsequent forensic search of the laptop found over 4,750 images of child pornography and 538 child pornography videos.

Phillips was indicted for one count of transportation of child pornography, in violation of 18 U.S.C. § 2252A(a)(l), and one count of possession of child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B). He moved to suppress the evidence from the laptop on the ground that, because Sawyer directed Windes to access Phillips's computer without his permission to show Sawyer what she had already seen, Windes's search of the computer at the sheriff's office was an unlawful law-enforcement search. After holding a hearing, the district judge denied the motion.

Phillips then entered a conditional guilty plea to one count of possessing child pornography, reserving the right to appeal the denial of his motion to suppress. Phillips was sentenced to 63 months' incarceration and 20 years of

supervised release subject to certain conditions that he also challenges on appeal.

DISCUSSION

The Supreme Court has long held that it does not violate the Fourth Amendment for a law enforcement officer to accept and use evidence that a private party discovers pursuant to its own private search, even if that private search was unlawful. *See Burdeau v. McDowell*, 256 U.S. 465, 475–76 (1921); *Coolidge v. New Hampshire*, 403 U.S. 443, 485–90 (1971). This rule is based on the principle that "[t]he Fourth Amendment[']s]protection against unlawful searches and seizures . . . applies to governmental action" and "was not intended to be a limitation upon other than governmental agencies." *Burdeau*, 256 U.S. at 475. Moreover, "the consequences of *Burdeau* do not offend the more modern rationale of the Fourth Amendment exclusionary rule . . . [which] is most often explained on grounds of deterrence." 1 Wayne R. LaFave, Search & Seizure § 1.8(a) (6th ed. 2021). Specifically, "extension of the exclusionary rule to all private illegal searches for purposes of deterrence would be difficult to justify" because "the private searcher . . . is often motivated by reasons independent of a desire to secure criminal conviction and . . . seldom engages in searches upon a sufficiently regular basis to be affected by the exclusionary sanction." *Id.*; *see also United States v. Janis*, 428 U.S. 433, 455 n.31 (1976) ("[T]he exclusionary rule, as a deterrent sanction, is not applicable where a private party . . . commits the offending act."). Still, "the issue of precisely what it takes to put a search outside the 'private' category is frequently litigated in a wide variety of settings." 1 LaFave, *supra*, § 1.8.

This is one such setting. Windes, on her own volition, searched Phillips's laptop and uncovered child pornography.

While she may not have had the authority to conduct the search on that password-protected laptop, she was clearly acting as a private party. Having discovered child pornography, and thus finding herself in possession of contraband, she decided to take and show it to law enforcement authorities. And when she was informed by a law enforcement officer that she should access the computer so that he could see what she wanted to show him, he made it clear that he did not wish to see anything more than what she had already seen, and she acted in line with those instructions.

1

Phillips asserts that Windes acted as a state agent when she completed the second search because she took cues from Sawyer when doing so. This argument is premised on Sawyer's effort to ensure that in viewing the materials that Windes had already seen and wished to show him, there would be no greater invasion of Phillips's privacy than had already occurred. Because the U.S. Attorney does not dispute Phillips's somewhat counterintuitive assertion that Windes acted as a state agent when she accessed the computer at the sheriff's office, we assume that this was a government search.

Nevertheless, this search was permissible. *United States v. Jacobsen* illustrates "the appropriate analysis of a governmental search which follows on the heels of a private one." 466 U.S. 109, 115 (1984). There, FedEx employees opened a package, saw it contained a white powdery substance, repacked the materials, and alerted the Drug Enforcement Administration ("DEA"). *See id.* at 111. Then, a DEA agent reopened the package, removed its contents without obtaining a warrant, and found that the white powder it contained was cocaine. *See id.* at 111–12. The Supreme

Court held that the FedEx employees' earlier private search and their decision to alert law enforcement to their findings made the agent's warrantless search permissible. The Court explained that "the legality of the governmental search must be tested by the scope of the antecedent private search." *Id.* at 116. "[I]t hardly infringed respondents' privacy for the [DEA] agent to reexamine the contents of the open package" because "the Federal Express employees had just examined the package and had, of their own accord, invited the federal agent to . . . view[] its contents." *Id.* at 119; *see id.* at 120 ("Similarly, the removal of the plastic bags from the tube and the agent's visual inspection of their contents [were permissible actions because they] enabled the agent to learn nothing that had not previously been learned during the private search."). We have thus held that *Jacobsen* establishes that, where a private party notifies law enforcement of its private search, a state "agent's [subsequent] search is permissible, and constitutional, to the extent that it mimic[s the earlier] private search." *United States v. Bowman*, 215 F.3d 951, 956, 963 (9th Cir. 2000).

That is precisely what occurred here. Windes went to the sheriff's office to alert law enforcement to what she uncovered on Phillips's laptop. Sawyer testified that he told Windes to "[j]ust do what you had done and show me what you saw." Windes testified that she "opened up the computer and turned it on, used the same password to log into Phillips'[s] user name, and then opened up the same Phone folder." She then scrolled down and showed him "the same files that [she] saw" the previous night with the same names that she had remembered. *Id.* She "did not access anything that [she] had not previously seen." A video was also admitted into evidence of Sawyer recreating the search he conducted with Windes, which showed that she did not have to "scroll down very far in the 'phone' folder before locating

the thumbnails corresponding to the filenames and descriptions he included in his search warrant affidavit." Based on this evidence, the district court judge found that "Sawyer told [Windes] to not show him anything she had not already seen, she understood his instruction, and she did not show anything she had not already seen." Indeed, the judge "infer[red]" from Sawyer's admonition that "Sawyer was aware of the private search exception and was trying to operate within it."

Although it is possible that—unlike a stagnant container—the folder on Phillips's computer could have automatically updated with new material from his phone between Windes's searches at her home and the sheriff's office or that a previously unviewed notification or alert could have popped up on the screen, Phillips does not allege that his devices were set to do so. Indeed, he concedes that the scope of the two searches was the same. Accordingly, we accept the district court's conclusion that, when Windes accessed the child pornography on Phillips's computer at the sheriff's office, she merely "mimicked [her earlier] private search." *Bowman*, 215 F.3d at 963.[1]

2

Nevertheless, Phillips argues that the evidence uncovered pursuant to Windes's actions at the sheriff's office must be suppressed for reasons tied to law

[1] Even if Sawyer had inadvertently seen more of Phillips's computer than Windes originally had, at least one circuit has held—as then-Judge Sotomayor explained—that "only the information attributable to that *additional* 'search' would require suppression," not the information the private individual already uncovered. *United States v. $557,933.89, More or Less, in U.S. Funds*, 287 F.3d 66, 87–88 (2d Cir. 2002) (Sotomayor, *J.*) (emphasis in original).

enforcement's subjective knowledge. For example, Phillips argues that *Jacobsen* does not apply because: "Sawyer lacked virtual certainty a subsequent search of Phillips's computer would reveal *only* contraband" or "virtual certainty that a subsequent search of the item [would] compromise no remaining privacy interest"; and "Sawyer did not know the details of Windes's [prior] search or full contents of the folder" containing the child pornography before Windes accessed the computer in his presence.[2] Phillips relies on language in the Supreme Court's decision in *United States v. Jacobsen*—language that we repeated in *United States v. Young*, 573 F.3d 711 (9th Cir. 2009). But neither case ultimately supports his arguments.

As Phillips points out, *Jacobsen* states that "[w]hen the first federal agent on the scene initially saw the package, he knew it contained nothing of significance except a tube containing plastic bags and, ultimately, white powder" and that, "[e]ven if the white powder was not itself in 'plain view,' . . . there was a virtual certainty that nothing else of significance was in the package and that a manual inspection of the tube and its contents would not tell him anything more than he already had been told." 466 U.S. at 118–19; *see id.* at 120 n.17 ("[T]he precise character of the white powder's visibility to the naked eye is far less significant than the facts that the container could no longer support any expectation of privacy, and that it was virtually certain that it contained nothing but contraband.").

But read in context, *Jacobsen*'s "virtual certainty" references—and other similar language—do not create any

[2] Phillips argues that, before Windes accessed the computer in Sawyer's presence, she had only told Detective Dickson what she had found and Dickson had not relayed that information to Sawyer.

subjective requirements for the application of its holding. Instead, the language to which Phillips points simply articulates an objective test pertaining to the scope of the searches. The Court described the DEA agent's prior knowledge of the entire package, as conveyed by the Fedex employees, because that knowledge made clear that the package had already been thoroughly examined and thus the government search could not exceed the scope of those employees' prior one. Indeed, the Court went on to explain:

> Respondents do not dispute that the Government could utilize the Federal Express employees' testimony concerning the contents of the package. If that is the case, it hardly infringed respondents' privacy for the agents to reexamine the contents of the open package by brushing aside a crumpled newspaper and picking up the tube. The advantage the Government gained thereby was merely avoiding the risk of a flaw in the employees' recollection, rather than in further infringing respondents' privacy. Protecting the risk of misdescription hardly enhances any legitimate privacy interest, and is not protected by the Fourth Amendment.

Id. at 119. The Court's explanation confirms that a government search that does not exceed the bounds of a private one is not an invasion of privacy under the Fourth Amendment. The only advantage gained by the government's own search is avoiding the private party's "misdescription"—and that is a permissible advantage. What was important to the *Jacobsen* Court was that the DEA agent's search "enabled [him] to learn nothing that had not previously been learned during the private search," not that

he have subjective knowledge of what was learned during the private search. The description of the DEA agent's knowledge simply made clear that he was not exceeding the private search. *Id.* at 120; *see also id.* at 116 ("[T]he legality of the governmental search must be tested by the scope of the antecedent private search."). "As in other Fourth Amendment contexts," then, the inquiry remains "an objective one." *Graham v. Connor*, 490 U.S. 386, 397 (1989); *cf. Torres v. Madrid*, 141 S. Ct. 989, 998 (2021) ("[W]e rarely probe the subjective motivations of police officers in the Fourth Amendment context.").

Here, as in *Jacobsen*, Windes's accessing the computer in Sawyer's presence "enabled [Sawyer] to learn nothing that had not previously been learned during the private search" and was therefore permissible. *Id.* at 120. But unlike *Jacobsen*, our conclusion regarding the equivalence between the scope of the searches arises because the record demonstrates that Sawyer instructed Windes to recreate her prior search so he only saw what she had already seen, and Windes abided by those instructions.[3]

Our opinion in *Young*, 573 F.3d 711, does not change this conclusion. It simply represents an application of the Supreme Court's decision in *Stoner v. California*, 376 U.S. 483 (1964). *Stoner* held that "[n]o less than a tenant of a

[3] Moreover, even if *Jacobsen*'s application depends on the subjective knowledge of the person conducting the search, that test was satisfied here. Unlike the DEA agent in *Jacobsen*, who had not conducted the initial search but who had learned about the entire contents of the package from the FedEx employees, Windes had previously accessed the Phone folder of Phillips's computer and saw that it contained child pornography. Thus Windes—the alleged state agent conducting the subsequent search in this case—possessed subjective knowledge and virtual certainty of what her search would reveal.

house, . . . a guest in a hotel room is entitled to constitutional protection" from a warrantless entry into his room regardless of any prior intrusion or permission given by hotel employees. *Id.* at 490. In *Young*, hotel security initially entered the defendant's room without his permission to investigate whether he had stolen items from another guest, and they uncovered a gun in his backpack in addition to other items. 573 F.3d at 714. This was a private search that did not implicate the Warrant Clause of the Fourth Amendment. Nevertheless, the issue in *Young* turned on a second entry into and search of the hotel room by hotel security after they contacted law enforcement officers. *Id.* at 715. "The Government d[id] not dispute the district court's conclusion that [hotel] security should be considered state actors for the purposes of the second search." *Id.* at 717. Thus, *Young* involved a warrantless entry into the defendant's hotel room by state actors against which he was protected by the Warrant Clause because "a hotel guest's . . . room is like a home . . . [and the] guest has a legitimate and significant privacy interest . . . against unlawful government intrusions." *Id.* at 721. And, absent exigent circumstances, such an intrusion is unlawful if undertaken without a warrant or consent of the occupant. *See Stoner*, 376 U.S. at 489–90; *see also Payton v. New York*, 445 U.S. 573, 589–90 (1980) ("[A]t the very core of the Fourth Amendment stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion. . . . Absent exigent circumstances, that threshold may not reasonably be crossed without a warrant." (alterations and internal quotation marks omitted)).

The language in *Young* upon which Phillips relies appears in our discussion rejecting "[t]he Government['s] argu[ment]," which it had raised "for the first time on appeal, that *United States v. Jacobsen* . . . should be extended to

permit the search of Young's backpack stored in his hotel room." 573 F.3d at 720. Phillips is correct that in *Young* we discussed language from *Jacobsen* that, by the time the DEA agent arrived, "it was virtually certain that [the package] contained nothing but contraband." *Jacobsen*, 466 U.S. at 120 n.17; *see Young*, 573 F.3d at 721. But when we did so, it was merely to explain that *Young* "[wa]s distinguishable from *Jacobsen" because the hotel security* "could not have been 'virtually certain' . . . that the gun was contraband." *Id.* After all, unlike narcotics, "[i]t is not a crime in most circumstances for a non-felon to possess a gun." *Id.*

While the two cases were distinguishable in the manner *Young* suggested, it is unlikely this distinction was crucial to our decision. Surely, we did not mean to suggest that our decision would have been different had the hotel security in *Young* been "virtually certain" as to the nature of the items the second search of Young's hotel room would uncover. Indeed, it could not have been. Unlike this case, *Young* concerned the unique privacy interests an individual has in his residence (and, by extension, a temporary residence like a hotel room). *See United States v. Lichtenberger*, 786 F.3d 478, 484 (6th Cir. 2015) ("Homes are a uniquely protected space under the Fourth Amendment."). Under *Stoner*, no prior private search and no level of certainty regarding what the second search would uncover could have allowed state actors to enter Young's hotel room without a warrant or his consent. *Young* relied expressly on well-settled Supreme Court law that "[b]elief, *however well founded*, that an article sought is concealed in a dwelling house, furnishes no justification for a search of that place without a warrant. And such searches are held unlawful notwithstanding facts unquestionably showing probable cause." 573 F.3d at 721 (emphasis added) (quoting *Johnson v. United States*,

333 U.S. 10, 14 n.14 (1948))).[4] Unlike *Young*, but like *Jacobsen*, this case does not involve a warrantless entry into a home or its equivalent. Accordingly, *Young* does not alter the current inquiry.

Phillips also argues that the extensive amount of personal information contained in a laptop makes it similar to a private residence, meaning that the private search doctrine should not apply. An analysis of this argument depends on to which of the two aspects of the doctrine it refers. The first involves an intrusion—even an extraordinarily invasive intrusion—by a private party who gives the contents discovered pursuant to that intrusion to law enforcement. *Burdeau v. McDowell*, 256 U.S. at 475–76. The validity of this conduct does not depend on the extent of the private information contained in the object or location on which the private party intruded. If there is no state action, there is no Fourth Amendment violation. *Id.*

By contrast, the second aspect of the private search doctrine involves "a governmental search which follows on the heels of a private one," *Jacobsen*, 466 U.S. at 115, and it is to this aspect of the doctrine that Phillips's argument refers. While it is true that modern computers contain so much personal information that a search of one could

[4] The leading treatise on the Fourth Amendment cites *Young* correctly for the proposition that "it is to be doubted that if a private person searched the premises of another and then reported to police what he had found . . . that the police could then make a warrantless entry of those premises and seize the named evidence." 1 LaFave, *supra*, § 1.8(b) & n.97. Indeed, *Young* was guided by the analytic framework of the Sixth Circuit in *United States v. Allen*, 106 F.3d 695, 698–99 (6th Cir. 1997), which specifically rejected the argument that *Jacobsen* could permit a "warrantless search of [a defendant's] motel room." *See Young*, 573 F.3d at 720–21.

"expose to the government far *more* than the most exhaustive search of a house," *Riley v. California*, 573 U.S. 373, 396 (2014), and more than the private party had previously uncovered, we have already held that the private search doctrine does apply to them, *see United States v. Tosti*, 733 F.3d 816 (9th Cir. 2013). We note that unlike in *Riley*, which involved a search incident to arrest, the search here involved a clear limiting principle: the private search exception allows police to review only the material that a private actor has already viewed. Because a digital container like "an email account, cell phone, or laptop" is composed of many smaller containers, a subsequent government search of a single file (or even a number of files) will not frustrate an individual's privacy interest in the entire device. *United States v. Wilson*, 13 F.4th 961, 977 n.13 (9th Cir. 2021). We acknowledge that it may be more difficult to have "virtual certainty" that a search of an electronic device does not reveal more than the private search had already revealed, given the dynamic nature of such devices. *See United States v. Rivera-Morales*, 961 F.3d 1, 13 (1st Cir. 2020) ("The Court did not define 'virtual certainty,' and it is not immediately apparent how that concept translates from the context of a static object like a package to the ever-changing screen on a cellphone."); *see also Lichtenberger*, 786 F.3d at 488. In this case, however, all parties agree that the officer did not see anything more than Windes had previously viewed, so we need not address this issue.

3

Phillips additionally argues that the Supreme Court's decision in *United States v. Jones*, 565 U.S. 400 (2012), supports reversing the district court's decision. In *Jones*, police attached a GPS tracking device to a car owned by the defendant's wife without a valid warrant. *Id.* at 402–03. The

district court denied the defendant's motion to suppress the data the police collected from that device, holding that the defendant lacked a reasonable expectation of privacy with respect to the car's movements on public streets. *Id.* at 403. The Supreme Court disagreed. It explained that, even if the defendant lacked a reasonable expectation of privacy with respect to the car's public movements, the Fourth Amendment nonetheless prohibited the police from physically trespassing on the defendant's wife's car by installing and using the tracking device without a valid warrant, and the exclusionary rule applied to the fruits of that unwarranted trespass. *Id.* at 404–06.

According to Phillips, *Jones*'s "common-law trespassory test" for Fourth Amendment violations requires suppression in this case. *Id.* at 409. *Jacobsen*, Phillips says, merely stands for the proposition that a private search eliminates an individual's reasonable expectation of privacy with respect to an item's contents. Thus, the fact that Windes had previously viewed the files containing child pornography on Phillips's computer only eliminated his reasonable expectation of privacy with respect to those files. It did not, Phillips argues, give Sawyer the license to instruct Windes to again "physically intrude[]" on Phillips's property—*i.e.*, his computer—by "open[ing] the laptop computer, enter[ing] the password . . . navigat[ing] to the 'phone folder' and scroll[ing] through the images." And, under *Jones*, that intrusion violated Phillips's Fourth Amendment rights.

This argument fails. Even if we attribute Windes's action to the officers and assume that those actions constituted a "trespass" of Phillips's property, *Jacobsen*, too, involved a trespass of the defendant's property. There, after the FedEx employees had opened the defendant's package and found

white powder, the DEA agent reopened the package and removed its contents. Yet the Supreme Court permitted the warrantless search even though the agent physically intruded onto the package. *See Jacobsen*, 466 U.S. at 118–22. *Jacobsen* thus establishes that law enforcement officers do not violate the Fourth Amendment when, as Phillips claims occurred here, they mimic the trespass a private individual visited on another's possessions after being alerted to the information uncovered pursuant to that trespass. *See Bowman*, 215 F.3d at 956, 963. *Jones* did not involve any aspect of the private search exception, nor did it reference *Jacobsen*. Under these circumstances, we must follow the Supreme Court's instruction that "if a precedent of this Court has direct application in a case, yet appears to rest on reasons rejected in some other line of decisions, the Court of Appeals should follow the case which directly controls, leaving to this Court the prerogative of overruling its own decisions." *Agostini v. Felton*, 521 U.S. 203, 237 (1997) (internal quotation marks and citation omitted).

Moreover, our decision in *Tosti*, which postdates *Jones*, is consistent with our rejection of Phillips's argument. There, a computer technician uncovered child pornography on the defendant's computer and alerted the police. *Tosti*, 733 F.3d at 818–19. When two detectives arrived, without first obtaining a warrant, one of them "directed [the technician] to open the images in a 'slide show' format so that they would appear as larger images viewable one by one." *Id.* at 819. The technician then "opened up the individual images" as the detective requested. *Id.* We held that, in light of the technician's prior search, *Jacobsen* dictated that these actions did not violate the defendant's Fourth Amendment rights. *Id.* at 821–22. Thus, we applied *Jacobsen* even though the technician, at the "direct[ion]" of the detective, arguably physically intruded on the defendant's computer

when he "opened up the individual images." *Id.* at 819. If *Jacobsen* applied in *Tosti*, it must also apply here.

Indeed, this case may be a stronger case than *Tosti* for applying *Jacobsen*. When Windes, acting as a private person, discovered the child pornography on Phillip's computer, she had at least two options for bringing it to the attention of law enforcement. First, and impracticably, she could have entered the sheriff's office with laptop open and the child pornography displayed in plain view. Second, she could have entered with the laptop closed and waited until she was in a private setting before opening the laptop and navigating to the child pornography. Sensibly, she chose the second option. And the only direction she received from a law enforcement officer was aimed at ensuring that she would not intrude on Phillips' privacy more than she already had.

In *Coolidge v. New Hampshire*, the Supreme Court observed in analogous circumstances that had the defendant's wife "wholly on her own initiative, sought out her husband's guns and clothing and then taken them to the police station to be used as evidence against him, there can be no doubt under existing law that the articles would later have been admissible in evidence." 403 U.S. at 487 (citing *Burdeau*, 256 U.S. 465). Phillips argues that because Windes chose the second option, the evidence uncovered pursuant to her actions at the sheriff's office must be suppressed. "[I]t would seem strange" if the result in "cases of this kind . . . [would] 'turn on the fortuity' of whether and to what extent the private person put the contents back into [or closed] the container before the police appeared," 1 LaFave, *supra*, § 1.8(b) (quoting *Jacobsen*, 466 U.S. at 120 n.17).

Tosti's application of *Jacobsen* to permit "the warrantless searches of [the defendant's] computer," *id.* at

821–22, also disposes of Phillips's argument, which we have already addressed, that "given the significant privacy interests implicated by modern digital devices, [*Jacobsen*] is categorically inapplicable to warrantless searches of these devices, such as Phillips's personal computer." *Cf. United States v. Wilson*, 13 F.4th 961, 972 (9th Cir. 2021) (declining to extend *Jacobsen* to a case where, in response to a Google report that its algorithm detected a match between images the defendant had attached to an email and known child pornography, "the government agent viewed [the] email attachments even though no Google employee—or other person—had done so"). Other circuits have also applied *Jacobsen* to searches of modern digital devices. *See United States v. Castaneda*, 997 F.3d 1318, 1327–29 (11th Cir. 2021); *Rivera-Morales*, 961 F.3d at 8–11; *United States v. Reddick*, 900 F.3d 636, 638–39 (5th Cir. 2018); *Lichtenberger*, 786 F.3d at 483–84; *United States v. Goodale*, 738 F.3d 917, 921 (8th Cir. 2013); *Rann v. Atchison*, 689 F.3d 832, 836–37 (7th Cir. 2012).

Phillips's objections to the use of evidence obtained from his computer therefore all fail.

We also reject Phillips's challenge to three conditions of his supervised release. Because Phillips signed a valid appeal waiver, he may argue on appeal only that those conditions "exceed[] the permissible statutory penalty [for the crime] or violate[] the Constitution." *United States v. Watson*, 582 F.3d 974, 981 (9th Cir. 2009). Yet our precedents establish the legality of all the challenged conditions. *See United States v. Gibson*, 998 F.3d 415, 422–23 (9th Cir. 2021) (risk notification), *cert. denied*, No. 21-6465 (Jan. 10, 2022); *United States v. Ochoa*, 932 F.3d 866, 869–71 (9th Cir. 2019) (prohibiting access to material depicting sexually explicit conduct involving adults to

defendant convicted of child pornography offense); *United States v. Stoterau*, 524 F.3d 988, 1003–04 (9th Cir. 2008) (polygraph testing).

The judgment of conviction is **AFFIRMED**.

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

* * *

UNITED STATES OF AMERICA, Plaintiff, v. DAREN W. PHILLIPS, Defendant.	Case No. 3:18-cr-00101-MMD-CBC-1 ORDER

I. SUMMARY

Defendant Daren W. Phillips was charged with transporting and possessing child pornography based on images found on a laptop his estranged ex-fiancée hacked into while he was in a residential substance abuse treatment center. His ex-fiancée brought the laptop into the Washoe County Sheriff's Office ("WCSO"), where she showed some of the images to a detective, who determined the images were likely child pornography, held onto the laptop, and later got a warrant to further search it. Before the Court is Defendant's motion to suppress the images as the unconstitutional fruit of a warrantless search, primarily arguing the search warrant was invalid because it depended on the warrantless joint search at the WCSO ("Motion").[1] (ECF No. 17.) The Court held an evidentiary hearing on the Motion on April 25 and 26, 2019 (the "Hearing"), and considers

[1]Per various stipulations between the parties, Defendant filed an errata and two supplements to his Motion. (ECF Nos. 18, 22, 27.) The government also filed a response to the Motion. (ECF No. 35.) Defendant did not file a reply. Per the Court's requests at the Hearing, the government and Defendant both filed status reports (ECF Nos. 58, 61), the government filed a video showing how Detective Sawyer saw the filenames he included in the search warrant affidavit for the laptop (ECF No. 60), and both Defendant and the government filed supplemental briefs addressing the applicable law in greater detail (ECF Nos. 62, 63).

the arguments raised and exhibits admitted therein. (ECF Nos. 54, 56.) Because the challenged searches all derive from the ex-fiancée's private search of the laptop, and the joint search with the WCSO detective did not exceed the scope of her private search—and for the reasons discussed below—the Court will deny the Motion.

II. FACTUAL FINDINGS

The Court relies on evidence attached to the parties' briefs, as well as the testimony presented at the Hearing,[2] to make its findings of fact. The Court points out any inconsistencies between the evidence before the Court where such inconsistencies are material to the Court's findings of fact.[3]

Defendant is a former Army Ranger and member of the Army reserve in Sacramento, California. (ECF No. 18 at 2.) He was engaged to marry Amanda Windes in the first half of 2018, but she decided to call off the engagement and kick him out of her house. (*Id.*) Specifically, Windes changed her mind because she thought Defendant had lied about being an alcoholic, was making poor financial decisions, and she found naked pictures of other adult women on one of his phones. (*Id.*) After Windes kicked him out of the house, the Veterans' Administration facilitated Defendant's placement in a one-month program at Bristlecone Family Resources, a mental-health and substance abuse residential treatment center. (*Id.*) Windes testified that she brought Defendant to Bristlecone, and helped him gather his belongings in anticipation of his stay there. There was a laptop amongst Defendant's belongings. Defendant's laptop ended up at Windes' house as a result of her helping him get his belongings together. The laptop stayed at Windes house while she went on a business trip, and Defendant was at Bristlecone.

According to Windes, while she was on this business trip, Defendant's ex-wife, with whom Defendant had daughters, reached out to Windes on Facebook Messenger

---

[2]Many of the Court's factual findings derive from testimony given at the Hearing. If a fact appears in this section without a citation, the fact comes from Hearing testimony.

[3]Fed. R. Crim. P. 12(d) provides: "Where factual issues are involved in determining a motion, the court must state its essential findings on the record."

because she had heard Defendant had entered Bristlecone, and was concerned that he would stop making child support payments for one of their daughters. (*See also* ECF No. 35 at 1-2.) Windes and Defendant's ex-wife exchanged several messages on Facebook Messenger. Apparently motivated by the fact that Windes also has daughters, Defendant's ex-wife told Windes in the course of this correspondence that she suspected Defendant had viewed child pornography in the past. (*Id.* at 2, 2 n.2) Further, Defendant's ex-wife recounted an incident where she caught Defendant fixated on her daughter's friends through a window during a pool party, where he may have been masturbating. (*Id.*) This conversation made Windes suspicious. (*Id.* at 2.)

The night she returned from her business trip, Windes decided to see what was on the laptop. (ECF No. 18-1 at 17.) Windes testified she was primarily motivated to look through the laptop to see if she could find additional evidence of bills Defendant had not been paying, but was secondarily motivated by a desire to see if he had been using the laptop to contact other women, and if, as his ex-wife had suggested, he was using it to view child pornography. As far as she knew, Defendant was the only person who had ever used the laptop. (*Id.* at 18.)

When she turned the laptop on, she found that it was password-protected. (ECF No. 18 at 2.) She knew a few of his Netflix passwords because she had gotten them from him in the past. (*Id.*; *see also* Defendant's Exhibit 12 admitted at the Hearing, a video recording of Windes' interview at the WCSO ("Exh. 12.").) She unsuccessfully tried to access the laptop using several of his Netflix passwords. (*Id.*) When that failed, she initiated the laptop's password recovery process. (*Id.*) She successfully guessed the answers to the two security questions presented to her as part of that process—the first by guessing Defendant chose 'sex' as his answer to a question prompting him for one of the 'greatest moments of his life,' and the second by trying one of the Netflix passwords again. (*Id.* at 2-3.) At this point, the laptop's password recovery process allowed Windes to send a temporary password to an email address. (*Id.* at 3.) She had the temporary password sent to her own email address. (*Id.*) Windes was able to log into Defendant's

computer with the temporary password she obtained, and then reset his password to something she could remember. (*Id.*)

While browsing around the contents of Defendant's laptop, she opened a folder on the desktop titled "phone." (ECF No. 18-1 at 17.) That folder contained hundreds of thumbnails of what appeared to her to be child pornography. (*Id.*) Windes testified that she scrolled all the way to the bottom of the 'phone' folder as it was displayed to her during this search. However, she also said that the folder contained several subfolders, which she did not open. In general, Windes testified that she scrolled through the whole folder, but did not open up every image and video file, and could not specifically remember which specific image or video files she had looked at. Regardless, she testified, after a while—she had seen enough. What she saw looked to her like child pornography, in part because various filenames indicated the ages of each photo or video's participants, and the thumbnails appeared to show children of those ages. Windes further testified that she saw nothing but child pornography in the 'phone' folder. Alarmed, Windes contacted campus police at the University of Nevada, Reno—she is employed there and has a working relationship with the campus chief of police. (ECF No. 18 at 3.) They directed her to contact WCSO. (*Id.*)

Windes brought the laptop to the front desk at WCSO on April 23, 2018. (ECF No. 18-1 at 17.) A WCSO front desk employee, Frank Cruz Torres, had Detective Arick Dickson come out and talk to her. Torres had Windes write the password to the laptop on a sticky note that he stuck on the front of the laptop, and took the laptop from her. Dickson had Windes meet him in the victim's room of WCSO's Detective Division. Dickson testified that he interviewed Windes in the victim's room for over two hours. He video recorded the interview. (*Id.* at 18.) In the interview, Windes told Dickson how and why she had hacked into Defendant's laptop, and about what she had found on it. (*Id.*; *see also* Exh. 12.)

At the conclusion of the interview, Dickson got the WCSO's victim's advocate to come speak with Windes in the victim's room, and the two spoke for some time. Dickson then came back into the victim's room with Detective Gregory Sawyer. They had the

laptop with them. Though the victim's room contained video recording equipment, neither Dickson nor Sawyer video recorded what happened next.

Sawyer asked Windes to show him what she had done to view the images and videos she stated were on the laptop, and told her "not to look anywhere different than where she had already seen the child pornography files." (ECF No. 18-1 at 17.) Sawyer affirmed during his testimony that he provided this instruction–that he "told her to show me what she had done, but not go any further…" Windes testified she understood Sawyer's instructions, and did not show him anything she had not already looked at. Sawyer also admitted during the Hearing that he did not know exactly what he would see when Windes turned the laptop on, and conceded he might have seen other information beyond child pornography that Windes had already looked at when she opened the computer, but did not.

Regardless, Windes complied with Sawyer's request by turning on the laptop[4] and entering a password when prompted to access an account Sawyer could see had the username "Daren Phillips." (*Id.*) Windes then opened a folder on the desktop titled "phone," which contained a number of thumbnails of images and videos that appeared to Sawyer to be child pornography. (*Id.*) While Windes does not remember Sawyer taking notes as they scrolled through the "phone" folder together, Sawyer testified he jotted down some file names and descriptions of the images and videos he saw on a piece of paper—though he later destroyed those notes.[5] Sawyer testified that, because of his experience with this type of work, he recognized some of the images and videos, which helped him to quickly conclude that the laptop contained child pornography. Again, both Sawyer and Windes consistently testified at the Hearing that Sawyer did not see anything Windes had

[4]Sawyer also testified that only Windes turned on the laptop, and that he had not turned on the laptop while it was out of Windes' sight, even though Windes had turned over the laptop to the WCSO with the password written on a post-it note.

[5]Sawyer testified that this is how he was able to include specific filenames and descriptions in his affidavit in support of his application for a search warrant to search the laptop.

not already seen during this search that occurred at the WCSO. After somewhere between two and around fifteen minutes,[6] Sawyer confirmed to Windes that the laptop likely contained child pornography, so he shut down the laptop, told Windes he was seizing it, and that he would get a search warrant to search its contents. (*Id.* at 18.)

Sawyer then applied for a search warrant to search the laptop's contents the next day, which was granted by Magistrate Judge William G. Cobb—that same day, April 24, 2018. (*Id.* at 20.) Sawyer's application for this warrant contained two written examples of specific pieces of content he viewed on the laptop, including the file name and a brief written description of each file's content. (*Id.* at 17-18.) At some point thereafter, Officer Robbie Hight conducted a forensic examination of the laptop that revealed numerous images and videos of alleged child pornography. (ECF No. 22-1 at 14; *see also* ECF No. 18 at 4.)

Sometime after April 24, 2018, Defendant called Windes from Bristlecone and asked her to retrieve the registration from his truck. (ECF No. 35 at 1-2.) She said she would. (*Id.* at 2.) When she searched through his truck for the registration, Windes found a second cell phone she was not previously aware Defendant owned. (*Id.*) She testified that this phone's number was only one digit different from the phone number of the phone she knew Phillips owned. Suspicious, she took it from the truck. (*Id.*) She turned it on and discovered it was fully charged. She testified that the phone's photo gallery contained many pornographic images. Because some of the women in the images looked young to Windes, she was concerned that the phone, like the laptop, also contained child

[6]At the Hearing, Sawyer said the entire interaction including the joint search of the laptop lasted around two minutes, Dixon said it was maybe five, and Windes said it was around fifteen. Based upon the duration of time it took Sawyer to demonstrate what Windes had done to power on the laptop, and then open the 'phone' folder on the home screen (ECF No. 60), the interaction was likely longer than the two minutes that Sawyer recalled. However, even though Sawyer's estimate that the interaction was as brief as two minutes is likely incorrect, it does not affect the Court's evaluation of Sawyer's credibility in light of the overall consistency between Sawyer and Windes' testimony about the interaction.

pornography. She further testified that she tried to call and email Sawyer about what she should do with the phone, but he did not respond.

Both because she was frustrated Sawyer was not responding to her attempts to contact him, and because she did not want the phone in her house, on June 25, 2018, Windes returned to the WCSO with the phone, and left it for Sawyer at the front desk. (ECF No. 22-1 at 14.) Sawyer testified he did not come down and talk to her that day because he was worried it would look like Windes was acting as an agent of the government, though she was acting entirely on her own. Nonetheless, at some point thereafter, Sawyer seized the phone as evidence. (*Id.* at 15.) On February 14, 2019, Sawyer applied for a search warrant to search the phone. (*Id.* at 9.) This warrant application contained four written examples of specific pieces of content found on the laptop—not the phone—two of which were not included in the search warrant application for the laptop. (*Id.* at 13; *see also* ECF No. 18-1 at 17-18.) Sawyer explained at the Hearing that the new examples he provided came from Hight's forensic examination of the laptop pursuant to the first search warrant authorized by Judge Cobb. Magistrate Judge Carla Baldwin Carry granted the search warrant application to search the phone that same day—February 14, 2019.[7] (ECF No. 22-1 at 2.)

III. DISCUSSION

This Motion raises important questions about how the private search exception to the Fourth Amendment's warrant requirement should be applied to digital devices that hold "the privacies of life[;]" "[w]ith all they contain and all they reveal." *Riley v. California*, 573 U.S. 373, 403 (2014) (citation omitted). The Court is also concerned that, drawn too broadly, the private search exception would allow the government to use evidence collected illegally by private citizen-vigilantes against other citizens in a way that would

[7]It is unclear if anything of evidentiary value was located on the phone. (ECF No. 22 at 1 n.1, 4.) Nonetheless, the government reserves the right to introduce evidence from the phone "depending on how the trial goes and what defense Mr. Phillips may raise." (ECF No. 58 at 2.) Therefore, the Court addresses the phone as well as the laptop in this order.

intrude upon those citizens' ever-diminishing and constitutionally-protected privacy rights. Thus, the Hearing was lengthy, and the Court requested and received supplemental briefing and evidence from the parties. However, under governing law, the facts before the Court on this Motion do not warrant suppression. Sawyer and Windes offered consistent, unrebutted testimony that the scope of the second search at the WCSO did not exceed the scope of Windes' earlier private search. As further explained below, the Court will therefore deny the Motion—both as to the laptop and the phone.

Defendant's primary argument in his Motion is that Windes' reconstructed search of the laptop with Sawyer at the WCSO violated his Fourth Amendment rights because it was undertaken at Sawyer's direction without a warrant. (ECF No. 17 at 5.) Defendant further argues that, when stripped of information gathered during the WCSO search, the affidavit submitted in support of the search warrant lacked sufficient factual information for Judge Cobb to find probable cause permitting further search of the laptop. (*Id.*)

The government counters there was no Fourth Amendment violation under the private search exception to the warrant requirement because Windes searched the laptop first, without direction from the government, and her reconstructed WCSO search did not exceed the scope of her initial private search. (ECF No. 35.) Defendant, in turn, responds to this argument by pointing to details included in the affidavits submitted in support of both search warrants that suggest Sawyer conducted a broader search of the laptop than Windes did—along with aspects of Windes and Sawyer's Hearing testimony—which would potentially bring the WCSO search outside the scope of the private search exception to the warrant requirement. (ECF Nos. 22 at 5.) Defendant buttresses his argument that suppression is warranted in arguing the laptop deserves heightened Fourth Amendment protection under recent Supreme Court cases (ECF No. 27 at 2-4), and because Sawyer did not know that the joint search he directed would remain within the scope of Windes' initial search—an argument based on the "virtual certainty" test

described by the Sixth Circuit in *United States v. Lichtenberger*, 786 F.3d 478 (6th Cir. 2015) (ECF No. 27 at 4-5).[8]

The Fourth Amendment protects citizens against unreasonable searches and seizures. *See, e.g.*, *U.S. v. Jacobsen*, 466 U.S. 109, 113 (1984). But "[t]he Fourth Amendment's proscriptions on searches and seizures are inapplicable to private action." *United States v. Tosti*, 733 F.3d 816, 821 (9th Cir. 2013) (citing *Jacobsen*, 466 U.S. at 113-114); *see also United States v. Sherwin*, 539 F.2d 1, 6 (9th Cir. 1976) ("A private person cannot act unilaterally as an agent or instrument of the state; there must be some degree of governmental knowledge and acquiescence. . . . In the absence of such official involvement, a search is not governmental. . . . And once a private search is completed, the subsequent involvement of government agents does not retroactively transform the original intrusion into a governmental search.") (citations omitted).

Thus, when a private actor conducts a search yielding potentially incriminating information, the defendant's original expectation of privacy protecting that information is deemed frustrated, and the government can use it without violating the Fourth Amendment, and without first obtaining a warrant. *See Tosti*, 733 F.3d at 821. "Instead, the Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated." *Id.* (quoting *Jacobsen*, 466 U.S. at 117) (internal quotation marks omitted). Therefore, "[t]he additional invasions of [a defendant's] privacy by the government agent must be tested by the degree to which they exceeded the scope of the private search." *Id.* (quoting *Jacobsen*, 466 U.S. at 115,

[8]Defendant makes an unpersuasive additional argument the Court will briefly address here. Defendant argues that the forensic examination of the laptop was not completed within the time period specified in the search warrant. (ECF No. 17 at 9.) The government persuasively counters that the forensic examination of the laptop was not untimely because the search warrant specified it could be completed as permitted under Fed. R. Crim. P. 41 (e)(2)(A). (ECF No. 35 at 15.) Fed. R. Crim. P. 41 (e)(2)(B) provides that "[u]nless otherwise specified, the warrant [issued under (e)(2)(A)] authorizes a later review of the media or information consistent with the warrant." Thus, the Court rejects Defendant's argument that the forensic examination of the laptop was untimely.

119). The key question before the Court is thus whether the joint search at the WCSO exceeded the scope of Windes' initial search of Defendant's laptop after hacking into it. *See id.*

The unrebutted testimony the two key witnesses—Sawyer and Windes—offered at the Hearing establishes that the second search at the WCSO did not exceed the scope of Windes' earlier private search.[9] Sawyer both testified at the Hearing and included in his search warrant affidavit that he instructed Windes to show him only what she had already seen, and nothing else.[10] (ECF No. 18-1 at 17.) Windes confirmed in her testimony that Sawyer told her to not show him anything she had not already seen, she understood his instruction, and she did not show him anything she had not already seen. And nothing presented at the Hearing causes the Court to question Sawyer or Windes' credibility.

Further, Windes testified she scrolled all the way to the bottom of the 'phone' folder during her first private search, so she at least glanced at everything in it, though she did not open the subfolders it contained. In the video recreating Sawyer's arguable joint search with Windes, consistent with Windes and Sawyer's testimony, Sawyer does not scroll down very far in the 'phone' folder before locating the thumbnails corresponding to the filenames and descriptions he included in his search warrant affidavit as to the laptop. (ECF No. 60 (third attempt, from around 4:00 to 6:00).) He certainly does not scroll all the way to the bottom of the folder as Windes testified she had done during her earlier private search, and does not need to open any subfolders to see these thumbnails. In addition, the thumbnails depict what appear to be children engaged in sexual acts, and the

[9]Neither party argues that Windes' first search of the laptop at home was anything but a purely private search. She also affirmed in her testimony at the Hearing that the decision to hack into Defendant's laptop was hers alone.

[10]The Court infers from this that Sawyer was aware of the private search exception and was trying to operate within it when Windes presented herself, unannounced, at the WCSO with a laptop that she said contained child pornography.

descriptive filenames are visible.[11] The Court also credits Sawyer's testimony that he was unfortunately familiar with some of the images he saw due to his experience working on the WCSO's crimes against children task force. Thus, it is believable that he would only need to see a few images before he decided to close the laptop, seize it, and apply for a warrant. In addition, there was also no testimony at the Hearing that Windes opened any subfolders and showed their contents to Sawyer. In sum, the evidence before the Court supports the government's argument that the scope of the second search was narrower than that of Windes' first private search.

That said, Defendant's counsel was able to elicit two strands of testimony from both Sawyer and Windes on cross-examination that get the closest of all the evidence—but neither shows that the scope of the second search was broader than the first. As to Sawyer, Defendant's counsel got him to admit on cross-examination that he had no idea what he would see when Windes opened up the laptop at his direction, including that he might see unrelated, private files. Indeed, Sawyer replied, "yes" to the question, "So, for you, there was no virtual certainty that the entire contents of that phone folder was going to be child pornography related?" But there is no dispute that Sawyer did not see anything other than pornography or child pornography when Windes opened up the laptop, and did not see any private, unrelated files. Further, these questions and responses do not go to the scope of the second search, but instead go to Sawyer's prospective knowledge, and thus do not directly affect the Court's analysis.

As to Windes, Defendant's counsel elicited testimony on cross-examination that she had not opened various subfolders within the 'phone' folder, and testimony to the effect that she was not sure exactly how many thumbnails she looked at during her private search, or which ones specifically. Similarly, she conceded she did not count the number

[11]Defendant points out in his supplemental brief that the reasonableness of the search is viewed through a prospective, not retrospective lens. (ECF No. 63 at 2-3.) But the Court is not making its decision through a retrospective lens. The point of Sawyer's exercise—recreating what the home screen and the 'phone' folder looked like when Windes first showed it to Sawyer—offers merely a demonstrative to illuminate Sawyer and Windes' testimony as to the extent of the arguable joint search.

of files in the 'phone' folder, nor could she say that she looked at a thumbnail of every single file in the folder. She also did not remember if she looked at the very last file at the very bottom of the 'phone' folder as it displayed on the laptop. However, none of this establishes that she showed Sawyer anything that she had not already seen, particularly when Sawyer and Windes' testimony evidences that Windes did not show Sawyer every file in the 'phone' folder—she had only showed him a few of the files starting from the top of the folder when Sawyer decided he had seen enough. And there is no dispute that she did not show him anything other than pornography or suspected child pornography, or anything outside of the 'phone' folder. Thus, the Court simply lacks any evidence that the scope of the second search exceeded the scope of the first sufficient to rebut Sawyer and Windes' consistent testimony that it did not.

Defendant argues that a Sixth Circuit case, *Lichtenberger*, 786 F.3d 478, announces a refined private search exception test more attuned to the digital world we live in which, when applied, suggests that the Court should grant the Motion here. (ECF No. 27 at 4-5.) The Court was intrigued by this argument, and allowed the parties to submit supplemental briefs on *Lichtenberger* that could also include any other recent cases addressing the difficult questions the Court faces here. (ECF Nos. 62, 63.)

Having reviewed those supplemental briefs, the Court is unpersuaded that *Lichtenberger* weighs in favor of a different result. First, *Lichtenberger* purports to either create a new private search exception test, or refine the existing one, but then does not apply that test—instead, the *Lichtenberger* court actually applies the more traditional scope test. *Compare Lichtenberger*, 786 F.3d at 488 ("To accomplish this, Officer Huston had to proceed with "virtual certainty" that the "inspection of the [laptop] and its contents would not tell [him] anything more than he already had been told [by Holmes.]") *with id.* at 491 ("we conclude that Officer Huston's warrantless review of Lichtenberger's laptop exceeded the scope of the private search Holmes had conducted earlier that day, and therefore violated Lichtenberger's Fourth Amendment rights to be free from an unreasonable search and seizure."). Second, the *Lichtenberger* court described its

decision as consistent with the law applied in the Ninth Circuit's governing decision in *Tosti*, which contains the test the Court applies in denying the Motion here. *See id.* at 490; *see also Tosti*, 733 F.3d at 822 (9th Cir. 2013) ("Even assuming that Detective Shikore viewed enlarged versions of the thumbnails, he still did not exceed the scope of Suzuki's prior search because Suzuki and both detectives testified that they could tell from viewing the thumbnails that the images contained child pornography."). Third, *Lichtenberger* is factually distinguishable in that there, neither the girlfriend nor the investigating officer were clear about the scope of either of the two searches, and whether the scope of the second exceeded the scope of the first. *See Lichtenberger*, 786 F.3d at 488 ("And Officer Huston himself admitted that he may have asked Holmes to open files other than those she had previously opened."). But here, Windes and Sawyer offered consistent, unrebutted testimony to the effect that the scope of the second search did not exceed the scope of the first private search. Thus, even if *Lichtenberger* bound this Court—and it does not—the Court does not find that applying *Lichtenberger* to these facts means the Court should grant the Motion.

In his supplemental, post-hearing brief, Defendant also argues that the Tenth Circuit's decision in *U.S. v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016), and the First Circuit's decision in *U.S. v. Powell*, Case No. 17-1683 (1st Cir. July 16, 2018) (ECF No. 63-1), weigh in favor of suppression. (ECF No. 63 at 3-4.) The Court is unpersuaded. As to *Ackerman*, then-judge Gorsuch found that the National Center for Missing and Exploited Children ("NCMEC") was a government actor, or alternatively was acting as a government agent, when one of its employees opened four images attached to an email AOL automatically forwarded to NCMEC based on an automatic determination that only one of those four images likely contained child pornography. *See Ackerman*, 831 F.3d at 1293-1304. Thus, *Ackerman* is distinguishable from this case, where Windes was unquestionably not acting as a government agent as to her first private search. Further, the *Ackerman* court found the private search doctrine entirely inapplicable. *See id.* at 1305-7. Here, the Court's decision is squarely within the private search doctrine. Finally,

while the *Ackerman* court declined to address the apparent applicability of the third-party doctrine to the facts of that case because the district court had not done so, it appears applicable because the defendant there sent the email through AOL, and thus *Ackerman* is further distinguishable from this case, where—surprisingly, as the Court is dealing with digital devices—the third party doctrine does not clearly apply. *See id.* at 1304-5; *see also id.* at 1308-9 (stating that the district court should consider the third-party doctrine on remand).

As to *Powell*, that court affirmed the district court's decision not to allow the defendant to withdraw his guilty plea based on ineffective assistance of counsel, because his trial counsel failed to file a motion to suppress, because the *Powell* court found he was unlikely to have succeeded on that motion to suppress had it been brought. (ECF No. 63-1 at 6-12.) More specifically, the First Circuit found (overlooking the potential applicability of the third party doctrine) that the private search doctrine applied, and would have resulted in denial of the defendant's hypothetical motion to suppress, while also rejecting a version of the 'digital is different' argument Defendant also advances here. (*Id.* at 9-12.) Thus, contrary to Defendant's suggestion, *Powell* actually weighs in favor of denying Defendant's Motion.

Defendant also argues the Court should adopt a requirement that police get a warrant before doing any search of a laptop even where, as here, the private search exception would otherwise apply—because 'digital is different.' (ECF No. 27 at 2-4.) To make this argument, Defendant relies on recent Supreme Court cases suggesting that digital devices deserve heightened Fourth Amendment protection. (*Id.*) The Court declines to adopt such a requirement. While the Court is persuaded by the broad contours of Defendant's argument on this point, it does not find the facts in this case merit an extension of existing law to impose a warrant requirement on Sawyer before he even looked at the laptop. To the Court's broad agreement with Defendant, the Court agrees that digital devices create special Fourth Amendment issues because of their immense storage capacity, internet connectivity, and citizens' tendency to store all details of our

personal lives on them, making those details easier to stitch together than they would have been in the past. *See Riley*, 573 U.S. at 393-97. But existing law does not impose the warrant requirement Defendant would like the Court to adopt here. *See Tosti*, 733 F.3d at 821. And the Court is not persuaded to extend the law under these facts—where Sawyer and Windes' unrebutted, consistent testimony establishing that the scope of the second search did not exceed the scope of the first, Sawyer appears to have been aware of the private search exception and appears to have attempted to rely on it in good faith, and there is no evidence of police misconduct or a lack of credibility on anyone's part that merits sending a cautionary Fourth Amendment message.

Defendant also argues that Windes may have committed a crime in hacking into Defendant's laptop, and seems to argue that should weigh in favor of suppression. (ECF No. 27 at 2.) However, whether Windes committed a crime is irrelevant to the private search exception analysis. Defendant has not cited, and the Court has not seen, a case standing for the proposition that the private search exception is not available to the government when the private actor violates a state or federal law in conducting the initial private search. Where, as here, the government was not involved in the initial private search, Defendant's Fourth Amendment rights were not violated by that initial search—regardless of its lawfulness. *See, e.g.*, *Jacobsen*, 466 U.S. at 115 ("The initial invasions of respondents' package were occasioned by private action. . . . Whether those invasions were accidental or deliberate, and whether they were reasonable or unreasonable, they did not violate the Fourth Amendment because of their private character.") (footnote omitted).

Both the government and Defendant make an additional argument that the Court finds unpersuasive, and thus non-dispositive of the Motion. First, the government argues that Defendant lacks standing to challenge the searches of the phone and the laptop because he has not admitted they were his. (ECF No. 35 at 3-4.) But Defendant stated at the Hearing that, for purposes of the Motion and the Hearing, the laptop and the phone are both his. And for the reasons the Court stated at the Hearing, the Court is

unpersuaded the standing argument is relevant or determinative. Second, Defendant argues that Windes could not legally consent—or have apparent authority to consent—to the WCSO search, so the consent exception to the warrant requirement does not apply here. (ECF No. 17 at 5-6.) But the government responds that the consent exception to the warrant requirement does not apply. (ECF No. 35 at 4-6.) Instead, as described above, the government argues that the private search exception is applicable here. (*Id.*) Therefore, whether Windes consented to the search of the laptop is not actually in dispute, or relevant to the Motion.

Because the Court will deny the motion as to any evidence on the laptop, the Court will also deny the motion as to any evidence recovered from the cellphone that Windes found in Defendant's truck and brought into the WCSO on June 25, 2018. Defendant's case for suppression was stronger as to the laptop than the phone, and having failed to persuade regarding the laptop, the Court sees no reason to suppress any evidence that may be on the phone. (*See* ECF No. 22 at 4 (arguing the phone should be suppressed for the same reasons the laptop should be suppressed).) First, Sawyer got a warrant before he even looked at the phone. Thus, in a sense, he complied with the requirement that Defendant would like to have imposed on him as to the laptop.

Second, to the extent Defendant continues to challenge the warrant as containing insufficient factual matter to support a probable cause finding (ECF No. 22 at 4-5), the Court is unpersuaded by that argument. A judge's probable cause determination is accorded "significant deference," *U.S. v. Gil*, 58 F.3d 1414, 1418 (9th Cir. 1995), and will be overturned only if it is "clearly erroneous." *U.S. v. Stanert*, 762 F.2d 775, 779 (9th Cir. 1985). Here, Defendant does not argue the affidavit submitted in support of the search warrant as to the phone contained misstatements or omissions. Instead, Defendant argues the affidavit submitted in support of the search warrant application as to the phone contained only details about the alleged child pornography found on the laptop, such that it could not establish probable cause as to the phone. (ECF No. 22 at 4-5.)

However, the affidavit as to the phone describes not only the alleged child pornography on the laptop, but the circumstances under which Windes found both the laptop and the phone, and brought them to WCSO at different times. (ECF No. 22-1 at 11-15.) As detailed in the affidavit, the fact that the alleged child pornography found on the laptop appeared in a folder called 'phone' supports the inference that there may also have been child pornography on the phone. (*Id.* at 12.) So too does the fact that Windes discovered a phone that she did not previously know existed, and the last time she discovered one of Defendant's digital devices, it was the laptop containing alleged child pornography.[12] (*Id.* at 14-15.) For these reasons, Judge Carry's issuance of the warrant as to the phone was not clearly erroneous. Therefore, to the extent the government intends to use it, the Court will not suppress any evidence gathered from the phone.

In sum, the Court will deny the Motion as to both the laptop and the phone. Most importantly, as to the laptop, Windes and Sawyer's testimony supports the Court's finding that the scope of the second search was narrower than Windes' first private search—and there is no persuasive evidence to the contrary.

///

///

///

///

///

///

///

///

///

[12]Though not directly relevant to this argument because it was not included in the affidavit submitted in support of the search warrant application as to the phone, Windes testified that the phone contained many pornographic images, some of which featured women that looked like underage children to her. Thus, without first examining each image very closely, Windes testified that she brought the phone to WCSO because she did not want it in her house, or to be responsible for it.

IV. CONCLUSION

The Court notes that the parties made several arguments and cited to several cases not discussed above. The Court has reviewed these arguments and cases and determines that they do not warrant discussion as they do not affect the outcome of the Motion.

It is therefore ordered that Defendant's motion to suppress (ECF No. 17) is denied.

DATED this 10th day of May 2019.

MIRANDA M. DU
UNITED STATES DISTRICT JUDGE