RECOMMENDED FOR FULL-TEXT PUBLICATION
Pursuant to Sixth Circuit I.O.P. 32.1(b)

File Name: 15a0095p.06

UNITED STATES COURT OF APPEALS

FOR THE SIXTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellant,

v.

ARON LICHTENBERGER,

Defendant-Appellee.

No. 14-3540

Appeal from the United States District Court
for the Northern District of Ohio at Toledo.
No. 3:12-cr-00570—James G. Carr, District Judge.

Argued: January 20, 2015

Decided and Filed: May 20, 2015

Before: MERRITT, STRANCH, and DONALD, Circuit Judges.

COUNSEL

ARGUED: Gene Crawford, UNITED STATES ATTORNEY'S OFFICE, Toledo, Ohio, for Appellant. Joel C. Bryant, UNIVERSITY OF MICHIGAN LAW SCHOOL FEDERAL APPELLATE LITIGATION CLINIC, Ann Arbor, Michigan, for Appellee. **ON BRIEF:** Gene Crawford, UNITED STATES ATTORNEY'S OFFICE, Toledo, Ohio, for Appellant. Joel C. Bryant, UNIVERSITY OF MICHIGAN LAW SCHOOL FEDERAL APPELLATE LITIGATION CLINIC, Ann Arbor, Michigan, Melissa M. Salinas, Gregory Geist, OFFICE OF THE FEDERAL PUBLIC DEFENDER, Toledo, Ohio, for Appellee.

OPINION

BERNICE BOUIE DONALD, Circuit Judge. This case deals with the suppression of evidence discovered during a private search and reviewed shortly thereafter by a police officer without a warrant. In 2011, defendant Aron Lichtenberger ("Lichtenberger") was arrested at the home he shared with his girlfriend, Karley Holmes ("Holmes"), for failing to register as a sex offender with the local authorities. After his arrest, Holmes hacked into Lichtenberger's personal laptop computer, where she discovered a number of images of child pornography. Holmes contacted the police, and when an officer arrived, Holmes showed the officer some of the images on the laptop. The officer then obtained a warrant for the laptop and its contents, which led to the present charges against Lichtenberger. Before trial, Lichtenberger filed a motion to suppress the laptop evidence, which the district court granted. The government appeals. As there are extensive privacy interests at stake in searches of a laptop, and as the officer had far less than "virtual certainty" regarding what he was going to see when Holmes showed him the results of her search, we **AFFIRM**.

I.

The facts, as presented in the district court's suppression order, are undisputed.

> On November 26, 2011, in the afternoon, Lichtenberger was with Karley Holmes, his girlfriend, at their shared home in Cridersville, Ohio. They lived there with Holmes's mother, who owned the residence. That day, two friends of Holmes's mother came over to the residence and told both Holmes and her mother that Lichtenberger had been previously convicted of child pornography offenses.
>
> One of the mother's friends then called the police. Several officers, including Douglas Huston, from the Cridersville Police Department[,] came to the residence. Holmes requested that the police escort Lichtenberger off the property because she did not want him living there anymore. Officer Huston determined that Lichtenberger had an active warrant for his arrest for failing to register as a sex offender, arrested him, and removed him from the property.
>
> Later that day, Holmes went into the bedroom she shared with Lichtenberger and retrieved his laptop. At the suppression hearing, she testified

> that she wanted to access his laptop because defendant "would never let me use it or be near him when he was using it and I wanted to know why." The laptop was password protected, but Holmes hacked the laptop by running a password recovery program. She then changed the password.
>
> Once she accessed the laptop, she clicked on different folders and eventually found thumbnails [*sic*] images of adults engaging in sexual acts with minors. She clicked on one of the thumbnails to see the larger image. When she found the first image, she took the laptop to the kitchen to show her mother. There, they clicked through several more sexually-explicit images involving minors. She closed the laptop and called the Cridersville Police Department.
>
> Officer Huston returned to the residence. In the kitchen, Holmes told the officer that she found child pornography on the defendant's laptop. She also told him that the laptop belonged to the defendant and that he was the only one who would access and use it. She explained that one time she tried to use the laptop and the defendant immediately became upset and told her to stay away from it. Lastly, Holmes told Officer Huston that she hacked the laptop to access it because it was password protected.
>
> Officer Huston then asked Holmes if she could boot up the laptop to show him what she had discovered. Holmes opened the laptop lid and booted it up to take it out of sleep mode. She then reentered the new password she created. Officer Huston asked her to show him the images. Holmes opened several folders and began clicking on random thumbnail images to show him. Officer Huston recognized those images as child pornography. He then asked Holmes to shut down the laptop.
>
> After consulting with his police chief over the phone, Officer Huston asked Holmes to retrieve other electronics belonging to Lichtenberger. She gave him Lichtenberger's cell phone, flash drive, and some marijuana. Officer Huston then left the premises with those items, the laptop, and its power cord.

United States v. Lichtenberger, 19 F. Supp. 3d 753, 754-55 (N.D. Ohio 2014). Holmes later testified that when she was reviewing Lichtenberger's laptop, she viewed approximately 100 images of child pornography saved in several subfolders inside a folder entitled "private."[1] Holmes also testified that she showed Officer Huston "a few pictures" from these files, although she was not sure if they were among the same images she had seen in her original search. Officer Huston testified that Holmes showed him "probably four or five" photographs.

[1] "They were in a folder marked 'private,' and when you clicked on the folder it came up with multiple other folders. And they were labeled with numbers that said two, three, four, five up to 12, and then when you clicked on one of those files, it came up with images in those individual files."

Lichtenberger was indicted on December 5, 2012, on three counts of receipt, possession, and distribution of child pornography under 18 U.S.C. §§ 2252(a)(2), (a)(4)(B), and (b). Before trial, Lichtenberger moved to suppress all evidence obtained pursuant to Officer Huston's warrantless review of the laptop with Holmes on November 26, 2011.[2] Lichtenberger argued that when Officer Huston directed Holmes to show him what she had found, Holmes was acting as an agent of the government such that the search was impermissible under the Fourth Amendment. The government countered that the review Officer Huston conducted was valid under the private search doctrine, which permits a government agent to verify the illegality of evidence discovered during a private search. Following a suppression hearing and additional briefing from the parties, the district court granted Lichtenberger's motion to suppress the laptop evidence. *Lichtenberger*, 19 F. Supp. 3d at 760. The government appeals.

II.

A.

In reviewing a district court's order to suppress evidence, we consider the district court's "conclusions of law and application of the law to the facts . . . de novo." *United States v. Bowers*, 594 F.3d 522, 525 (6th Cir. 2010) (quoting *United States v. Hardin*, 539 F.3d 404, 416 (6th Cir. 2008)) (internal quotation marks omitted). We review the district court's factual findings for clear error. *Id.*

B.

The private search doctrine originated from the Supreme Court's decision in *United States v. Jacobsen*, 466 U.S. 109 (1984). As with any Fourth Amendment case, the facts underlying the *Jacobsen* case are key to its holding. In 1981, Federal Express ("FedEx") employees were inspecting a package—a box wrapped in brown paper—that had been damaged in transit. *Id.* at 111. The employees opened the box and discovered that it contained a duct-tape tube about ten inches long nestled among wadded sheets of newspaper. *Id.* The employees removed the tube from the box and cut a slit in the end of the tube. *Id.* Inside, they found

[2]Lichtenberger initially sought to suppress other evidence, as well, but the government responded that it did not intend to present the other evidence at trial. Suppression of the laptop was the sole issue before the district court when it issued its order of April 30, 2014. *Lichtenberger*, 19 F. Supp. 3d at 754 n.1. It remains the sole issue on appeal.

multiple zip-lock bags of a white, powdery substance. *Id.* The employees placed the bags back in the tube, put the tube back in the box, and called the Drug Enforcement Administration ("DEA"). *Id.* A DEA agent arrived and found the box open on a desk. *Id.* The agent observed that the tube inside had a slit cut into it, and removed the bags from the tube. *Id.* He then opened each bag and removed a trace amount of the powder for an on-site field test. *Id.* at 111-12. The test positively identified the substance as cocaine. *Id.* at 112. Based on the agent's findings, the DEA procured a warrant to search the place to which the package had been addressed and subsequently arrested the defendants. *Id.*

The question before the Supreme Court was whether the DEA agent's search of the package and field test of its contents—both conducted without a warrant—violated the Fourth Amendment. If so, the package and any evidence obtained pursuant to the warrant based on its contents were inadmissible. The Court began with the fundamental principle that the Fourth Amendment protects "an expectation of privacy that society is prepared to consider reasonable." *Id*. at 113. When a government agent infringes on this reasonable expectation, a "search" occurs for the purposes of the Fourth Amendment, and the government must obtain a warrant or demonstrate that an exception to the warrant requirement applies. However, the Fourth Amendment only protects against "governmental action; it is wholly inapplicable 'to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official.'" *Id*. at 113-14 (quoting *Walter v. United States*, 447 U.S. 649, 662 (1980) (Blackmun, J., dissenting)); *see also id.* at 115 ("The initial invasions of [defendants'] 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).

Applying these principles, the Supreme Court distinguished between the invasion of privacy that resulted from the FedEx employees' search of the package and the invasion that resulted from the DEA agent's subsequent review, because "[o]nce frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-nonprivate information." *Id*. at 117. The Court held that, in a situation where "a

governmental search . . . follows on the heels of a private one[,]" "[t]he additional invasions of [a person's] privacy by the government agent must be tested by the degree to which they exceeded the scope of the private search." *Id*. at 115. In other words, the government's ability to conduct a warrantless follow-up search of this kind is expressly limited by the scope of the initial private search. *Id*. at 116 ("[T]he Government may not exceed the scope of the private search unless it has the right to make an independent search.").

The Court therefore analyzed whether the DEA agent's after-occurring search had exceeded the scope of the FedEx employees' initial search of the package. The Court found that the agent's removal of the cocaine from the package remained within the scope—and was therefore permissible under the Fourth Amendment—because he was merely confirming what the employees had told him and there was a "virtual certainty" that he was going to find contraband and little else in the package. *Id*. at 118-20 (footnote omitted) (citing *Coolidge v. New Hampshire*, 403 U.S. 443, 487-90 (1971) and *Burdeau v. McDowell*, 256 U.S. 456, 475-76 (1921)). The Court then evaluated whether the cocaine field test conducted by the agent exceeded the scope of the initial private search and found that it had because the FedEx employees had taken no similar action. *Id*. at 121. However, the Court concluded that the field test—which would merely confirm or refute that the powder was cocaine—could not disclose any facts in which the defendants had a legitimate privacy interest protected by the Fourth Amendment, and was therefore independently permissible to the extent it exceeded the scope of the initial private search. *Id*. at 122-26.

C.

1.

As discussed, the government argues that Officer Huston's review and subsequent seizure fall within the ambit of the private search doctrine as articulated by *Jacobsen*. Lichtenberger argues that this Court's holding in *United States v. Allen*, 106 F.3d 695, 699 (6th Cir. 1997), prevents application of the private search doctrine in his case. In *Allen*, we declined to extend

the private search doctrine to an after-occurring search of a motel room—"a temporary abode containing personal possessions" that is akin to a home.[3] *Id*. We explained that,

> [u]nlike the package in *Jacobsen* . . . which "contained nothing but contraband," Allen's motel room was a temporary abode containing personal possessions. Allen had a legitimate and significant privacy interest in the contents of his motel room, and this privacy interest was not breached in its entirety merely because the motel manager viewed some of those contents. *Jacobsen*, which measured the scope of a private search of a mail package, the entire contents of which were obvious, is distinguishable on its facts; *this Court is unwilling to extend the holding in* Jacobsen *to cases involving private searches of residence*s.

Id. at 699 (emphasis added).

Lichtenberger argues that, because the laptop was in his home and because laptops may contain private information similar to that in a home, our holding in *Allen* prevents application of the private search doctrine to his case. While there is good reason to be concerned about the breadth of private information contained in a laptop—*see infra*—Lichtenberger's argument goes a step too far. Homes are a uniquely protected space under the Fourth Amendment, and that protection "has never been tied to measurement of the quality or quantity of information obtained." *Kyllo v. United States*, 533 U.S. 27, 37 (2001). Rather, any and all details in a home "are intimate details, because the entire area is held safe from prying government eyes." *Id.* The fact remains that Officer Huston did not search Lichtenberger's home. We decline to extend the protection afforded to homes to a laptop computer.

The parties do not dispute that Holmes acted solely as a private citizen when she searched Lichtenberger's laptop, that she invited Officer Huston into a common area of the residence she and Lichtenberger shared (the kitchen), and that she then showed the officer a sample of what she had found. The district court found that this fact pattern was analogous to the critical elements of *Jacobsen*—a private search followed closely by a governmental search—and held

[3]The facts of *Allen* are these. In 1993, the defendant checked into a motel. *Allen*, 106 F.3d at 697. After he failed to pay his bill, the manager entered his room and discovered large amounts of marijuana in plain view. *Id*. The manager left the room, locked it with a master key only she possessed, and called the police. *Id.* When officers arrived, the manager opened the door for them and let them enter the room while she remained outside. *Id*. The officers viewed the room for about fifteen seconds and observed not only the marijuana, but also the handle of a pistol that was in plain sight. *Id.* Officers subsequently arrested the defendant and a jury convicted him of possession of marijuana with intent to distribute and possession of a firearm during a drug trafficking crime. *Id*. at 697-98. On appeal, the defendant argued that the officers' search of his motel room violated the Fourth Amendment, and that any evidence derived therefrom was inadmissible. The government responded that the officers' actions were permissible under the private search doctrine. We disagreed. *Id.* at 699.

that the private search doctrine applied in this case. We agree. This case presents an after-the-fact confirmation of a private search. Accordingly, *Jacobsen* properly applies, as the district court found. *Lichtenberger*, 19 F. Supp. 3d at 757.

2.

Having found that Holmes' initial search was private and that *Jacobsen* governs, the district court erred in its ensuing analysis. Instead of proceeding to an analysis of the scope of Officer Huston's search vis-a-vis Holmes' private search, the court addressed Lichtenberger's argument that Holmes was acting as an agent of the government when she showed Officer Huston photographs on the laptop. The district court found:

> The protections of the Fourth Amendment do not apply to a search or seizure "effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any government official." . . . Thus, I must determine whether Holmes acted as an agent of Officer Huston. If she did, I must suppress the laptop as evidence.

Id. at 758 (quoting *Jacobsen*, 466 U.S. at 113).

Because Holmes re-opened the laptop and navigated its contents at Officer Huston's behest, the district court found that Holmes had acted as an agent of the government. *Id*. at 759 (relying on *United States v. Robinson*, 390 F.3d 853, 872 (6th Cir. 2004)). Under this agency analysis, the court held that Officer Huston's review of the photographs constituted an impermissible warrantless search under the Fourth Amendment, and granted Lichtenberger's motion to suppress on that basis. *Id*. at 759-60.

While we agree with the district court's conclusion, we disagree with its approach. Though the district court properly found that *Jacobsen* governed the case at bar, the court did not apply the scope test articulated by the Supreme Court in that case. It is true that *Jacobsen* discusses the essential distinction between searches conducted by a government agent and those conducted by a private party, but that section of the opinion is dicta that clarifies why a government search may properly follow on the heels of a private search. 466 U.S. at 119-20.

Agency is relevant to Holmes' initial search because government involvement at that stage would remove the case from *Jacobsen*'s ambit entirely. *Id.* at 115 n.10 (noting that the justification for the private search conducted by FedEx was questioned in a post-trial affidavit, but because "lower courts found no governmental involvement in the private search, a finding not challenged by respondents[, t]he affidavit [was] thus . . . of no relevance[.]"); *see also Bowers*, 594 F.3d at 526 ("In this case, because it was wholly private action that first uncovered the [evidence], with neither involvement by law enforcement nor an intent to aid law enforcement, [the private searchers] cannot be considered government agents at the time that the [evidence] was discovered initially.") And agency is relevant to an after-occurring search analysis where the court determines that the after-occurring search exceeds the scope of the initial private search.[4] *Jacobsen*, 466 U.S. at 117-18 ("The Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated. In such a case the authorities have not relied on what is in effect a private search, and therefore presumptively violate the Fourth Amendment if they act without a warrant.") But it is only possible to evaluate the elements of a government search "that exceeded the scope of the initial private search" *after* those elements have been identified by comparing the scope of the two searches. Thus, in *Jacobsen*, the Supreme Court did not begin by determining the agency behind the officer's actions. *Id.* at 113-26. Rather, the Court first evaluated whether the officer's actions remained within the confines of the initial private search conducted by the FedEx employees who discovered the package. *Id.* After determining those limits, then the Court examined the elements of the officer's search that went beyond the FedEx employee's actions (namely, the cocaine test the officer conducted). *Id.* at 122 ("The question remains whether the additional intrusion occasioned by the field test, which had not been conducted by the Federal Express agents and therefore exceeded the scope of the private search, was an unlawful 'search' or 'seizure' within the meaning of the Fourth Amendment.") Accordingly, the correct inquiry is whether Officer Huston's search remained within the scope of Holmes' earlier one.

[4]In that instance, the government must show an independent justification for that element of the search exceeding the scope. This application of agency is evident in the facts of *Jacobsen*, wherein a DEA agent—acting openly in his role as a representative of law enforcement—conducted the after-occurring search in question. *Id.* at 113-26.

D.

We find that the scope of Officer Huston's search of Lichtenberger's laptop exceeded that of Holmes' private search conducted earlier that day. This is, in large part, due to the extensive privacy interests at stake in a modern electronic device like a laptop and the particulars of how Officer Huston conducted his search when he arrived at the residence.

We evaluate "[t]he reasonableness of an official invasion of the citizen's privacy . . . on the basis of the facts as they existed at the time that invasion occurred." *Jacobsen*, 466 U.S. at 115. Under the private search doctrine, the critical measures of whether a governmental search exceeds the scope of the private search that preceded it are how much information the government stands to gain when it re-examines the evidence and, relatedly, how certain it is regarding what it will find. *Id*. at 119-20 (finding the DEA agent's search permissible because "there was a virtual certainty that nothing else of significance was in the package[.] . . . 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."); *see also id.* at 117 ("This standard follows from the analysis applicable when private parties reveal other kinds of private information to the authorities. . . . The Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated.")

These principles have guided our application of the private search doctrine for three decades. We have held a government search permissible—that is, properly limited in scope—in instances involving physical containers and spaces on the grounds that the officers in question had near-certainty regarding what they would find and little chance to see much other than contraband. For instance, in *United States v. Bowers*, the defendant's roommate's boyfriend discovered a photo album containing what he believed to be child pornography in the defendant's bedroom dresser. 594 F.3d at 524. When the summoned authorities arrived at the defendant's home, his roommate directed them to the dining room table, where the agents opened the album to view the potentially incriminating evidence. *Id*. at 524-25. We upheld the agents' search of the photo album because the roommate had already described the contents of the album. *Id*. at 526. The agents therefore knew the album contained child pornography,

"learn[ed] nothing that had not previously been learned during the private search," and "infringed no legitimate expectation of privacy." *Id*. at 526 (quoting *Jacobsen*, 466 U.S. at 120) (internal quotation marks omitted). In *United States v. Richards*, we held that police entry into a storage unit containing images of child pornography was sufficiently limited under the private search doctrine because "[t]he officers merely confirmed the prior knowledge that [the private party] learned earlier in the day—that unit 234 contained child pornography." 301 F. App'x 480, 483 (6th Cir. 2008).

By contrast, we have declined to apply the private search doctrine where an officer's search of a physical space goes beyond the scope of the initial private search. In *United States v. Williams*, the defendants' landlord, after receiving a high water bill, entered their rental property to check for leaks. 354 F.3d 497, 500 (6th Cir. 2003). The landlord had only inspected the kitchen of the property before leaves strewn across the floor, a suspicious odor, and a lack of light or furniture in the residence convinced her to leave and call the DEA. *Id*. At the landlord's request, a DEA agent inspected the entire house for a water leak. *Id*. at 500-01. He found no leaks, but he did find a great deal of marijuana. *Id*. at 501. After assuming the space was not a residence[5] and contained "nothing but contraband," we found the government's search violated the Fourth Amendment because it infringed upon the defendants' constitutionally protected privacy interests and those interests had not already been frustrated by the landlord's incursion earlier that day. *Id*. at 510.

However, searches of physical spaces and the items they contain differ in significant ways from searches of complex electronic devices under the Fourth Amendment. On this point, we find the Supreme Court's recent decision in *Riley v. California*, 134 S. Ct. 2473 (2014), instructive. The *Riley* decision arose from two cases in which officers had found cell phones on the defendants during searches incident to arrest, secured and searched the data on those cell phones without warrants, and subsequently discovered evidence used against the defendants at trial. *Id*. at 2480-82. The *Riley* Court held that the search-incident-to-arrest exception, which permits law enforcement to search items found on a suspect's person or in a suspect's vehicle at the time of arrest without a warrant, did not extend to the data on a cell phone. *Id*. at 2485.

[5]We acknowledged in *Williams* that, were we to consider the structure a home, our holding in *Allen* would have also prevented application of the private search doctrine. *Id*. at 510.

Instead, the Court declared the searches unconstitutional, and emphasized that "officers must generally secure a warrant before conducting such a search." *Id.*

The *Riley* Court explained that, under the Fourth Amendment, "we generally determine whether to exempt a given type of search from the warrant requirement 'by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.'" *Id*. at 2484 (quoting *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999)). In the context of a search incident to arrest, that determination must be made by weighing the governmental interests of officer safety and preservation of evidence against the invasion of privacy inherent in searching the belongings someone has on their person at the time of arrest. *Id*. When the belonging in question is a device like a cell phone, the balance between governmental and privacy interests shifts enormously:

> [N]either of [these] rationales has much force with respect to digital content on cell phones. On the government interest side, [we have previously] concluded that the two risks identified. . . —harm to officers and destruction of evidence—are present in all custodial arrests. There are no comparable risks when the search is of digital data. In addition, [we have] regarded any privacy interests retained by an individual after arrest as significantly diminished by the fact of the arrest itself. Cell phones, however, place vast quantities of personal information literally in the hands of individuals. A search of the information on a cell phone bears little resemblance to the type of brief physical search considered in [our prior cases].

Id. at 2484-85 (discussing *United States v. Robinson*, 414 U.S. 218 (1973) and *Chimel v. California*, 395 U.S. 752 (1969)). The Court reasoned that "when privacy-related concerns are weighty enough[,] a search may require a warrant, notwithstanding the diminished expectations of privacy of the arrestee." *Id*. at 2488 (quoting *Maryland v. King*, 133 S. Ct. 1958, 1979 (2013)).

Of particular relevance to our inquiry, the Supreme Court discussed the particular qualities of electronic devices that must be considered. Cell phones, the Court noted, "are in fact minicomputers that also happen to have the capacity to be used as a telephone. . . . One of the most notable distinguishing features of modern cell phones is their immense storage capacity." *Id*. at 2489. That storage capacity

> has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.

Id. Thus, the likelihood that an electronic device will contain 1) many kinds of data, 2) in vast amounts, and 3) corresponding to a long swath of time, convinced the *Riley* Court that officers must obtain a warrant before searching such a device incident to arrest. *Id*.

We reach the same conclusion regarding the private search doctrine in the case at bar. As with any Fourth Amendment inquiry, we must weigh the government's interest in conducting the search of Lichtenberger's property against his privacy interest in that property. That the item in question is an electronic device does not change the fundamentals of this inquiry. But under *Riley*, the nature of the electronic device greatly increases the potential privacy interests at stake, adding weight to one side of the scale while the other remains the same. *Id*. at 2488.

This shift manifests in *Jacobsen*'s "virtual certainty" requirement. For the review of Lichtenberger's laptop to be permissible, *Jacobsen* instructs us that Officer Huston's search had to stay within the scope of Holmes' initial private search. 466 U.S. at 119. 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.]" *Id*. That plainly was not the case. As the district court found, "there was absolutely no virtual certainty that the search of Lichtenberger's laptop would have" revealed only what Officer Huston had already been told. *Lichtenberger*, 19 F. Supp. 3d at 759; *see also id*. ("[T]he search of a laptop is far more intrusive than the search of a container because the two objects are not alike. . . . [G]iven the amount of data a laptop can hold, there was absolutely no virtual certainty" as there was in *Jacobsen*.).

Considering the extent of information that can be stored on a laptop computer—a device with even greater capacity than the cell phones at issue in *Riley*—the "virtual certainty" threshold in *Jacobsen* requires more than was present here. When Officer Huston arrived, he asked Holmes to show him what she had found. While the government emphasizes that she showed Officer Huston only a handful of photographs, Holmes admitted during testimony that she could not recall if these were among the same photographs she had seen earlier because there were hundreds of photographs in the folders she had accessed. And Officer Huston himself admitted that he may have asked Holmes to open files other than those she had previously opened. As a result, not only was there no virtual certainty that Officer Huston's review was limited to the photographs from Holmes's earlier search, there was a very real possibility Officer Huston exceeded the scope of Holmes's search and that he could have discovered something *else* on Lichtenberger's laptop that was private, legal, and unrelated to the allegations prompting the search—precisely the sort of discovery the *Jacobsen* Court sought to avoid in articulating its beyond-the-scope test.

All the photographs Holmes showed Officer Huston contained images of child pornography, but there was no virtual certainty that would be the case. The same folders—labeled with numbers, not words—could have contained, for example, explicit photos of Lichtenberger himself: legal, unrelated to the crime alleged, and the most private sort of images. Other documents, such as bank statements or personal communications, could also have been discovered among the photographs. So, too, could internet search histories containing anything from Lichtenberger's medical history to his choice of restaurant. The reality of modern data storage is that the possibilities are expansive.

We are not alone in our approach to these modern considerations under the Fourth Amendment. Our sister circuit courts have placed a similar emphasis on virtual certainty in their application of *Jacobsen* to searches of contemporary electronic devices. In *United States v. Runyan*, the Fifth Circuit adopted a relatively broad approach when it partially excluded the fruits of a warrantless government search of computer disks alleged to contain child pornography. 275 F.3d 449, 464 (5th Cir. 2001). In that case, the defendant's ex-wife turned over a number of disks to police, but she had only viewed the contents of some of them. *Id*. at

453. Analogizing the various disks to opened and unopened containers, the court found that "the police exceed the scope of a prior private search when they examine a closed container that was not opened by the private searchers *unless the police are already substantially certain of what is inside* that container based on the statements of the private searchers, their replication of the private search, and their expertise." *Id*. at 463 (emphasis added). Where the defendant's ex-wife had previously viewed files on a disk and confirmed they contained child pornography, therefore, the court upheld the police's after-occurring inspection. *Id*. at 464. However, where the ex-wife had not viewed a disk, the police had no "substantial certainty" regarding their contents, and the court found that those searches violated the Fourth Amendment. *Id*.

A decade later, the Seventh Circuit applied the same rationale to uphold police review of similar evidence. In *Rann v. Atchison*, a 15-year-old victim of child pornography reported the defendant to the police. 689 F.3d 832, 834 (7th Cir. 2012). After the police interview, she went home and retrieved a memory card containing evidence to support her allegations. *Id*. The defendant's wife (and the victim's mother) later provided a computer zip drive with similarly incriminating evidence stored on it. *Id*. While the police reviewed both items without a warrant, the court held the after-occurring searches permissible under *Jacobsen* and *Runyan*:

> The Illinois Appellate Court specifically found that [t]his is not a case where multiple pieces of potential evidence were turned over to the police, who then had to sift through the potential evidence to discover if any factual evidence existed. To the contrary, in this case [the victim] turned exactly one memory card over to the police, and her mother gave the police exactly one zip drive. We cannot imagine more conclusive evidence that [the victim] and her mother knew exactly what the memory card and the zip drive contained.[6] . . . Likewise, even if the police more thoroughly searched the digital media devices than [the victim] and her mother did and viewed images that [the victim] or her mother had not viewed, per the holding in *Runyan*, the police search did not exceed or expand the scope of the initial private searches. *Because [the victim] and her mother knew the contents of the digital media devices when they delivered them to the police, the police were "substantially certain" the devices contained child pornography*.

[6]Specifically, the court found that the record supported the notion the victim's mother had actually saved the materials to the zip drive herself, making her knowledge of the evidence it contained far more comprehensive than Holmes' knowledge of the contents of Lichtenberger's laptop in the instant case. *Id*. at 837-38 (highlighting the Illinois Appellate Court's finding that "[a]lthough no testimony exists regarding how the images on the zip drive came to be there . . . it seems highly likely that [the victim]'s mother [compiled] the images on the zip drive herself, downloading them from the family computer," and holding that "the Illinois Appellate Court's factual findings are reasonable, and [defendant] has failed to present clear and convincing evidence—indeed, any evidence whatsoever—to overcome the presumption of correctness we give to the state court's finding.")

> Accordingly, the subsequent police search did not violate the Fourth Amendment, and Rann's ineffective assistance of counsel claim must fail.

Id. at 837-38 (internal quotation marks omitted) (emphasis added).

A case with similar concerns regarding police review of pornographic images on a laptop was recently decided by the Ninth Circuit, as well. In *United States v. Tosti*, the court found that an after-occurring search was permissible under *Jacobsen*, noting that:

> The district court explicitly found that Detective Shikore had viewed only those photos Suzuki had already viewed. Tosti does not contest that conclusion here, nor does the record contradict it. . . .
>
> 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. That is, the police learned nothing new through their actions. Since Suzuki—a private individual to whom Tosti had voluntarily delivered his computer with the explicit understanding that he would inspect the system to complete the repairs—could discern the content of the photos, any expectation of privacy Tosti had in those pictures was extinguished. Whether detectives later enlarged them (or the size of the enlargements, for that matter) is thus irrelevant.

733 F.3d 816, 822 (9th Cir. 2013). Unlike in the case at bar, the record in *Tosti* clearly established that Detective Shikore saw the exact same images as Suzuki had in a preceding private search. Here, we have a record that establishes the opposite: Holmes was not at all sure whether she opened the same files with Officer Huston as she had opened earlier that day. Other courts have conducted a similar analysis in parallel cases. *See*, *e.g.*, *United States v. Goodale*, 738 F.3d 917, 921 (8th Cir. 2013), *cert. denied*, 134 S. Ct. 2856 (2014); *cf. United States v. Odoni*, 782 F.3d 1226, 1238-39 (11th Cir. 2015).

We find that Officer Huston's lack of "virtual certainty" when he reviewed the contents of Lichtenberger's laptop is dispositive in this instance. However, we also note that, like the cases in *Riley*, the situation here lacked some of the risks that support an immediate search. *Riley*, 134 S. Ct. at 2486-88. The need to confirm the laptop's contents on-site was not immediate. Lichtenberger was nowhere near the premises, having been arrested earlier that day;

the images were not in danger of erasure, deterioration, or tampering. *Id*. at 2586 ("[O]nce law enforcement officers have secured a cell phone, there is no longer any risk that the arrestee himself will be able to delete incriminating data from the phone."). The laptop presented no cognizable, immediate threat to Officer Huston, Holmes, or anyone else when Officer Huston arrived at the Holmes residence to review it. *Id*. at 2485 ("Digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape. Law enforcement officers remain free to examine the physical aspects of a phone to ensure that it will not be used as a weapon[.]") These circumstances were knowable to Officer Huston at the time he arrived.

In light of the information available at the time the search was conducted, the strong privacy interests at stake, and the absence of a threat to government interests, 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. The laptop evidence and evidence obtained pursuant to the warrant issued on the basis of its contents must be suppressed.

III.

For the foregoing reasons, we **AFFIRM** the decision of the district court and **REMAND** the case for further proceedings consistent with this opinion.