UNITED STATES COURT OF APPEALS

FOR THE SECOND CIRCUIT

_____

August Term 2012

(Argued: November 19, 2012 Decided: June 25, 2013)

Docket No. 11-4808-cr

_____

UNITED STATES OF AMERICA,

Appellee,

— v. —

JAMES R. GALPIN, JR.,

Defendant-Appellant.

_____

Before:

JACOBS, *Chief Judge*, WINTER, *Circuit Judge*,
and SWAIN, *District Judge*.*

_____

Appeal, following conditional guilty plea, from denial of motion to suppress evidence indicative of guilt of child pornography-related offenses. Affirmed in part, and vacated and remanded in part.

_____

* The Honorable Laura Taylor Swain of the United States District Court for the Southern District of New York, sitting by designation.

JAMES P. EGAN (Lisa Peebles and James F. Greenwald on the brief) Federal Public Defender's Office, Northern District of New York, Syracuse, New York, *for Defendant-Appellant* James Galpin, Jr.

PAUL D. SILVER, Assistant United States Attorney (Richard S. Hartunian, United States Attorney, and Miroslav Lovric, Assistant United States Attorney, on the brief), Northern District of New York, Albany, New York, *for Appellee.*

SWAIN, *District Judge*:

Defendant-Appellant James R. Galpin, Jr. ("Galpin"), was convicted in the United States District Court for the Northern District of New York (*McAvoy, J.*) upon a conditional guilty plea, of several counts of production of child pornography, committing a felony offense involving a minor while being required to register as a sex offender, and possession of child pornography. He was sentenced on November 1, 2011, principally to 572 months of imprisonment. Prior to his guilty plea, Galpin had moved to suppress all of the evidence, including images of child pornography found on Galpin's computer, digital cameras, and digital storage devices, that had been seized in the execution of a search warrant that authorized officers to search for "evidence that will constitute, substantiate or support violations of NYS Corrections Law, section 168-f subdivision four, NYS Penal Law and or Federal Statutes."[1] The district court denied Galpin's motion in its entirety, holding that, although the warrant was overbroad and probable cause was lacking for its authorization to conduct a search for child pornography, the warrant was severable and the images that were found would have been in

[1] The cited Correction Law provision requires the registration of certain internet service provider and communications accounts. **[See infra note 2]**.

plain view during the execution of a properly limited search. Galpin appeals from the district court's November 2, 2011, judgment. We affirm the district court's determinations that the officers lacked probable cause to search for evidence of child pornography and that the warrant was facially overbroad. Because we find deficient the factual and analytical record as to whether the warrant was severable and whether the images of child pornography were seized in plain view, we vacate the judgment and remand the case for further proceedings consistent with this opinion.

BACKGROUND

The Underlying Investigation

Galpin was convicted in New York in 1991 of Sexual Abuse in the First Degree. He had abused 22 boys between the ages of 10 and 15. In June 2009, several years after his release from custody and following a tip from a "concerned citizen" who reported having seen Galpin with a young boy and calls from two parents reporting that Galpin had contacted their children, the Southern Tier Cyber Predator Task Force opened an investigation. Law enforcement officials in Tioga County, New York, installed a 24-hour surveillance camera outside of Galpin's residence. The surveillance revealed numerous boys between the ages of 10 and 16 visiting the residence and spending the night. The investigation also revealed that Galpin was communicating with at least one minor boy on the Internet social networking site "MySpace" using the screename "Medic Guy." Specifically, investigators found Galpin's photograph and the "Medic Guy" online identity posted on the MySpace page of a 13-year old boy, who was Galpin's relative. Upon discovering the posting, investigators reviewed Galpin's sex offender registration and learned that he had failed to register the "Medic Guy" identifier as

required by N.Y. Correction Law § 168-f.[2]

The Search Warrant

On July 6, 2009, Tioga County Sheriff's Department Senior Investigator Patrick Hogan ("Hogan") applied to the Owego Town Court for a warrant to search Galpin's residence, person, and vehicles for, inter alia, cameras, computers, cell phones, and any and all computing or data processing software, "which may reveal evidence which substantiates violations of Penal Law statutes, Corrections Law statutes and or Federal statutes." Warrant Appl. 1, July 6, 2009. In the warrant application, Hogan set forth the details of the investigation, including observed interactions and communications with young males, and the fact that an internet provider had revealed in response to a subpoena that the subscriber I.P. address associated with the "Medic Guy" posting belonged to Galpin.

Based on this information, Hogan concluded in his application that Galpin was "engaged in the use of the internet via MySpace and chat to lure juvenile males to the residence for the purpose of engaging in sexual conduct, . . . using [his] cell phone to make contact with and direct the pickup of juveniles, . . . [and] transport[ing] juvenile males to his residence." Warrant Appl. 2. Citing his training and experience, Hogan further proffered that "persons involved in child sexual exploitation use the internet, cell phones and practices of becoming

---

[2] N.Y. Correction Law § 168-f(4) provides, in relevant part, that: "Any sex offender shall register with the division [of criminal justice] no later than ten calendar days after any change of address, internet accounts with internet access providers belonging to such offender, [and] internet identifiers that such offender uses . . . ." "Internet identifiers" are defined as "electronic mail addresses and designations used for the purposes of chat, instant messaging, social networking or other similar internet communication." N.Y. Correct. Law § 168-a(18).

juvenile friendly to groom juveniles for the purpose of engaging in sexual behavior with children." Warrant Appl. 2. In addition, Hogan made the following claim:

> [I]t is reasonable to expect that upon execution of this warrant evidence will be obtained that James Galpin Jr. is using his computer or other device[s] capable of accessing the World Wide Web to include but not limited to computer's [sic], cell phones, game systems or ipod's [sic] capable of communicating with other persons, to post, chat, text, sending pictures or video's [sic], or talk live and evidence of such will be located at the residence or on the person, or vehicle of James Galpin, Jr.

Warrant Appl. 3. Finally, again citing his training and experience, Hogan asserted that "persons who engage in sexual predator behaviors do not provide current e-mail address's [sic], user names or passwords on their sexual offender registration to avoid detection of illegal activities by Law Enforcement and to divert Law Enforcement to a plausible or legitimate e-mail which do [sic] not contain any of the subjects [sic] illicit activities." Warrant Appl. 3.

Upon being presented with the application, Town of Owego Justice Robert W. Henning issued a warrant to search Galpin's residence, vehicle, and person for property "believed to contain evidence that will constitute, substantiate or support violations of NYS Corrections Law, section 168-f subdivision four, NYS Penal Law and or Federal Statutes." Warrant 1, July 6, 2009. More specifically, the warrant, which did not incorporate the application, authorized the seizure and subsequent search of:

> 1) Any Computers, central processing units, external and internal drives, storage units or media terminals and video display units, together with peripheral equipment such as keyboards, printers, modems, scanners or digital camera's [sic] and their internal or external storage media.
>
> 2) Any and all computing or data processing software, or data including but not limited to hard disks, floppy disks, magnetic tapes, intregal [sic] RAM or ROM units, and any other permanent or portable storage device(s) which may reveal evidence and substantiates violations of the aforementioned NYS and federal statutes.

3) The following records and documents, whether contained or stored on the computer, magnetic tape, cassette, disk, diskette, photo optical device, or any other storage medium:

a. Any access numbers, passwords, personal identification numbers (PINS), logs, notes, memoranda and correspondence relating to computer, electronic and voice mail systems, internet address's [sic] and/or related contacts.

b. Any computing or data processing literature, including, but not limited to printed copy, instruction books, notes, papers, or listed computer programs, in whole or in part.

c. Any audio or video cassette tape recordings, books magazines [sic], periodicals, or other recorded or printed material, the possession of which constitutes a violation of the aforementioned statutes of the Laws of New York state or Federal Statutes.

d. Any and all photographs depicting sexual conduct by a child and/or minors engaged in sexually explicit conduct.

e. Any records or correspondence relating to the possession, transmission, collection, trading or production of the aforementioned photographs.

Id.

Hogan executed the warrant on July 8, 2009. Among the items discovered were a computer and digital photography equipment that were found upon forensic examination to contain images of child pornography. On March 10, 2010, a grand jury handed up a nine-count indictment, charging Appellant with four counts of production of child pornography in violation of 18 U.S.C. § 2251(a) and (e), one count of possession of child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B), and four counts of committing a felony offense involving a minor, specifically the four production counts, while being required to register as a sex offender in violation of 18 U.S.C. § 2260A.

Galpin's Suppression Motion

On December 16, 2010, Galpin moved to suppress the evidence obtained and derived from the search warrant.[3] Galpin argued that investigators lacked probable cause to believe that he had committed any offense beyond failing to register an internet identifier, as required by N.Y. Correction Law § 168-f(4), and thus had no basis for conducting a broad search of the information contained on his computer and camera equipment. Galpin also argued that, by expansively referencing "NYS Penal Law and or Federal Statutes," the warrant authorized an impermissible general search. The government opposed the motion to suppress, arguing that the warrant application established probable cause to believe that Galpin was using the internet and cell phones to lure minors for sexual activity, and that he had failed to register the "Medic Guy" identifier that Galpin had used to contact a minor via MySpace. The Government also argued that, even if the warrant was invalid insofar as it authorized a search for pornographic images, such images were in plain view incident to the properly authorized search for evidence of a registration offense and luring, and that, in any event, investigators acted on the warrant in good faith, such that suppression was inappropriate under United States v. Leon, 468 U.S. 897 (1984).

On January 24, 2011, the district court held a suppression hearing, during which the court heard oral argument from counsel and examined the warrant and underlying application. Following the argument, the court made oral findings that "[t]he facts asserted in the warrant application establish that the defendant was using the internet, including posting images of himself online to communicate with minor males, in violation of the registration

[3] Galpin also requested a hearing pursuant to Franks v. Delaware, 438 U.S. 154 (1978). The district court denied that request and Galpin does not challenge that ruling.

requirements," and that it was "reasonable to conclude that engaging in such acts involved the use of a computer or other device with access to the internet . . . ." The court continued:

> [I]t was reasonable to conclude that relevant evidence would include any and all information concerning defendant's accessing the internet, including passwords and other documents or information concerning his accessing the internet and using screen names or accounts that he failed to register. This is because the defendant used the internet in furtherance of his failure to register. It similarly is reasonable to conclude that relevant evidence would include digital pictures that he may have uploaded or downloaded in furtherance of his efforts to locate and communicate with minor males under accounts that he did not register. Such evidence would be relevant to whether it was actually defendant who was using an unregistered user name or e-mail account.

The court also found that it was a "reasonable and logical inference to believe that persons who communicate with one another via the internet will share photographs, whether sexually explicit or not," emphasizing that it had been established that the "defendant did upload an image of himself to a minor's MySpace page, albeit not a sexually explicit photograph." The court concluded that it was "not a far leap to conclude that there may have been evidence of defendant uploading other pictures of himself or having downloaded pictures of the people he met online, including minors" and, therefore, that the warrant authorizing the search of computers and digital equipment for images was reasonable.

In addition, the district court found that there was probable cause to believe that Galpin was "grooming or luring minor males for inappropriate sexual conduct or had engaged in unlawful sexual conduct with a minor," based on the warrant affidavit's proffers concerning Galpin's criminal history, surveillance observation of overnight stays by young males in Galpin's home, internet and other communications with minor males, the presence of computer and massage equipment in Galpin's home, "his bringing minor males to his home in his vehicle[,] and his failure to register the user name that he was using to communicate with minor males."

The district court specifically found that the warrant application failed to establish probable cause to search for child pornography and upheld Galpin's overbreadth objection to the extent the warrant authorized searches for evidence of unspecified New York State Penal Code and Federal Law violations. The court concluded, however, that the invalid portions of the warrant could be "redacted" from the valid ones, and directed that a hearing would be held to determine whether the evidence of child pornography was seized in plain view during the execution of the search warrant.

Although the district court did not identify specifically the elements of the warrant that could be redacted or those that would remain, it observed that the "affidavit clearly discusses activity relating to defendant's failure to register and his attempting to lure minor males for sexual activity . . . [and that i]t, thus, appears that Hogan intended to look only for evidence relating to the failure to register and efforts by the defendant to lure minor males for purposes of sexual activity." The district court also found, subject to receipt of evidence as to the search methodology that had revealed the child pornography, that, "[c]onsidering the totality of the nature of the investigation, the documents in support of the warrant, and the warrant itself, the Court does not discern deliberate police misconduct in attempting to engage in a general search such that exclusion would be justified."

The Evidentiary Hearing

An evidentiary hearing in connection with the suppression motion was held on March 1, 2011. At the hearing, the government called Marsha Powell ("Powell"), a computer forensics analyst with the Computer Analysis and Technical Services lab of the Broome County Security Division. Powell testified that law enforcement officers had provided her with materials and information in support of their request that consisted of, inter alia, the warrant

affidavit and warrant contents, a timeline of activity in connection with the investigation, and of Galpin's post-warrant arraignment on 20 charges of a criminal sex act in the second degree, misdemeanor sexual abuse charges, and charges of forceable touching and endangering the welfare of a child. Powell testified that, in conducting her examination, she looked for files associated with the names of suspected minors who were listed in the timeline report and the "Medic Guy" identifier, as well as "images of a sexual nature if they involved what [she] thought might be underage males or younger males," and for "images that [she] believed would be of Mr. Galpin."[4] Before Powell conducted her examination of Galpin's computer, digital camera, and digital storage media, she learned that Galpin had accessed web sites, especially social networking sites such as MySpace. She testified that she knew that there might be images of Galpin on at least one of those web sites, and that the storage media might contain the names and images of potential male victims of Galpin's.

Powell explained that, in order to conduct the analysis of Galpin's computer and devices, she first made an image, or duplicate, of the hard drive. The forensic analysis was conducted on that duplicate. Powell began her examination of the computer by doing word searches for pertinent names based upon her review of the information provided to her. Once the initial word searches were completed, Powell segregated the types of files that had been identified as containing relevant information. These files were then opened and examined individually. Powell explained that each file on the hard drive contained an extension

---

[4] See also the district court's Decision and Order, United States v. Galpin, No. 10-110, slip op at 3 (N.D.N.Y. Mar. 3, 2011), ECF No. 33 ("Powell was looking for evidence of online communications between Defendant and minors and evidence that Defendant had shared digital photographs of himself with minors or obtained digital photographs of minors, which may have included pornography.").

corresponding to the type of associated file (e.g., "doc" for Microsoft Word documents or "jpeg" for image files). Powell testified that, while the file name signifies the file type, the name may bear no relationship to the file's content; therefore, the only way to determine the content is to open the file. As Powell reviewed the files, she bookmarked ones she deemed relevant to the investigation. In addition to searching all of the images and text files on the computer and storage media, Powell testified, she opened and viewed every video file. Powell admitted that, after she conducted a search of the hard drive for files containing certain terms, she conducted a search of the entire hard drive. During the search, Powell stated, she was looking for internet history showing child pornography, evidence of sexual abuse of children, evidence of communications with children, and "images of a sexual nature if they involved what [Powell] thought might be underage males or younger males."

On March 3, 2011, the District Court issued a written opinion denying Galpin's suppression motion. Crediting Powell's testimony, the district court found that the forensic examination of Galpin's computer required opening and viewing every file to determine whether it contained relevant content. In doing so, the district court found, Powell had inadvertently observed images of child pornography. Consequently, the district court held, the plain view doctrine applied because (1) the government had probable cause to search Galpin's computer for "images or other evidence concerning the sex offender registration violation"; (2) the discovery was inadvertent "in that Powell had to open each file to determine whether they fell within the scope of the warrant"; and (3) "the incriminating nature of the evidence was readily apparent by simply looking at the pictures and drawing logical inferences concerning the depictions therein."

The Plea and Aftermath

On March 9, 2011, Galpin entered a conditional plea of guilty to the nine-count indictment. The plea agreement preserved his right to appeal the district court's denial of his motion to suppress evidence. On November 2, 2011, the district court entered judgment sentencing Galpin principally to a 572-month term of imprisonment. Galpin filed a timely notice of appeal on November 10, 2011.

DISCUSSION

The standard of review for evaluating the district court's ruling on a suppression motion is clear error as to the district court's factual findings and de novo as to questions of law. United States v. Rodriguez, 356 F.3d 254, 257 (2d Cir. 2004). The evidentiary record is reviewed in the light most favorable to the government. United States v. Rosa, 626 F.3d 56, 61 (2d Cir. 2010).

I.

The Fourth Amendment to the Constitution of the United States provides that: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.

The chief evil that prompted the framing and adoption of the Fourth Amendment was the "indiscriminate searches and seizures" conducted by the British "under the authority of 'general warrants.'" Payton v. New York, 445 U.S. 573, 583 (1980); Arizona v. Gant, 556 U.S. 332, 345 (2009) ("[T]he central concern underlying the Fourth Amendment [is] the concern

about giving police officers unbridled discretion to rummage at will among a person's private effects."). To prevent such "general, exploratory rummaging in a person's belongings" and the attendant privacy violations, Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971), the Fourth Amendment provides that "a warrant may not be issued unless probable cause is properly established and the scope of the authorized search is set out with particularity." Kentucky v. King, --- U.S.---, 131 S. Ct. 1849, 1856 (2011).

The particularity requirement has three components. First, a warrant must identify the specific offense for which the police have established probable cause. See United States v. Bianco, 998 F.2d 1112, 1116 (2d Cir. 1993) (warrant that contained no particular description of items and made no mention of any criminal statute or criminal conduct was "not supportable"), abrogated on other grounds by Groh v. Ramirez, 540 U.S. 551 (2004); United States v. George, 975 F.2d 72, 76 (2d Cir. 1992) (warrant authorizing search for evidence "relating to the commission of a crime" was overbroad because "[n]othing on the face of the warrant tells the searching officer for what crimes the search is being undertaken").[5] Second, a warrant must describe the place to be searched. United States v. Voustianiouk, 685 F.3d 206,

[5] Mindful that the purpose of this requirement is to minimize the discretion of the executing officer, other Circuits have held that even warrants that identify catch-all statutory provisions, like the mail fraud or conspiracy statutes, may fail to comply with this aspect of the particularization requirement. See, e.g., United States v. Leary, 846 F.2d 592, 594 (10th Cir. 1988) (warrant authorizing search of export company's business records for violation of the "Arms Export Control Act, 22 U.S.C. § 2778, and the Export Administration Act of 1979, 50 U.S.C.App. § 2410," held overbroad); Voss v. Bergsgaard, 774 F.2d 402 (10th Cir. 1985) (warrant specifying 18 U.S.C. § 371, the general federal conspiracy statute, held overbroad); United States v. Roche, 614 F.2d 6, 8 (1st Cir. 1980) (concluding that a limitation of a search to evidence relating to a violation of 18 U.S.C. § 1341, the general mail fraud statute, provides "no limitation at all").

211 (2d Cir. 2012); 2 W. LaFave, Search and Seizure § 4.6(a) (5th ed. 2012) ("[G]eneral searches are prevented by the other Fourth Amendment requirement that the place to be searched be particularly described."). Third, the warrant must specify the "items to be seized by their relation to designated crimes." United States v. Williams, 592 F.3d 511, 519 (4th Cir. 2010); see also United States v. Buck, 813 F.2d 588, 590-92 (2d Cir. 1987) (finding that a warrant authorizing the seizure of "any papers, things or property of any kind relating to [the] previously described crime" failed the particularization requirement because it "only described the crimes – and gave no limitation whatsoever on the kind of evidence sought"). "[A]n otherwise unobjectionable description of the objects to be seized is defective if it is broader than can be justified by the probable cause upon which the warrant is based." 2 W. LaFave, Search and Seizure § 4.6(a) (5th ed. 2012).

In an oft-quoted passage, the Supreme Court has held that the particularity requirement "makes general searches . . . impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant." Marron v. United States, 275 U.S. 192, 196 (1927). To be sure, we have noted that this "no discretion" standard "has not always been applied literally," and that courts may tolerate some ambiguity in the warrant so long as "law enforcement agents have done the best that could reasonably be expected under the circumstances, have acquired all the descriptive facts which a reasonable investigation could be expected to cover, and have insured that all those facts were included in the warrant." United States v. Young, 745 F.2d 733, 759 (2d Cir. 1984). Nonetheless, we have emphasized that "a failure to describe the items to be seized with as much particularity as the circumstances reasonably allow offends the Fourth Amendment

because there is no assurance that the permitted invasion of a suspect's privacy and property are no more than absolutely necessary." George, 975 F.2d at 76.

Where, as here, the property to be searched is a computer hard drive, the particularity requirement assumes even greater importance. As numerous courts and commentators have observed, advances in technology and the centrality of computers in the lives of average people have rendered the computer hard drive akin to a residence in terms of the scope and quantity of private information it may contain.[6] See United States v. Payton, 573 F.3d 859, 861-62 (9th Cir. 2009) ("There is no question that computers are capable of storing immense amounts of information and often contain a great deal of private information. Searches of computers therefore often involve a degree of intrusiveness much greater in quantity, if not different in kind, from searches of other containers."); United States v. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009) (noting computer's potential "to store and intermingle a huge array of one's personal papers in a single place"); Orin Kerr, Searches and Seizures in a Digital World, 119 Harv. L. Rev. 531, 569 (2005) (Computers "are postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more."). The potential for privacy violations occasioned by an unbridled, exploratory search of a hard drive is enormous. This threat is compounded by the nature of digital storage. Where a warrant authorizes the search of a residence, the physical dimensions of the evidence sought will naturally impose limitations on where an officer may pry: an officer

---

[6] Tellingly, at the January 24, 2011, district court hearing, the government itself compared the hard drive search to a house search: "[the] search of a computer is no different than an officer searching various places in the home. An officer can't tell what's in the drawer or what's in the folder if he has or she has authority to look in those places."

could not properly look for a stolen flat-screen television by rummaging through the suspect's medicine cabinet, nor search for false tax documents by viewing the suspect's home video collection.[7] Such limitations are largely absent in the digital realm, where the size or other outwardly visible characteristics of a file may disclose nothing about its content.[8]

As the Ninth Circuit has explained, because there is currently no way to ascertain the content of a file without opening it and because files containing evidence of a crime may be intermingled with millions of innocuous files, "[b]y necessity, government efforts to locate particular files will require examining a great many other files to exclude the possibility that the sought-after data are concealed there." United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1176 (9th Cir. 2010) (en banc) (per curiam). Once the government has obtained authorization to search the hard drive, the government may claim that the contents of every file it chose to open were in plain view and, therefore, admissible even if they implicate the defendant in a crime not contemplated by the warrant. There is, thus, "a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." Id. This threat demands a heightened sensitivity to the particularity requirement in the context of digital searches.

---

[7] Cf. United States v. Ross, 456 U.S. 798, 824 (1982) (the scope of a lawful search is "defined by the object of the search and the places in which there is probable cause to believe that it may be found. Just as probable cause to believe that a stolen lawnmower may be found in a garage will not support a warrant to search an upstairs bedroom, probable cause to believe that undocumented aliens are being transported in a van will not justify a warrantless search of a suitcase.").

[8] See, e.g., United States v. Crespo-Rios, 645 F.3d 37, 43 (1st Cir. 2011) (recognizing that files may easily be manipulated through, inter alia, mislabeling to disguise their content); accord United States v. Hill, 459 F.3d 966, 977-78 (9th Cir. 2006).

II.

The district court determined, and the government does not dispute, that insofar as the warrant generally authorized officers to search Galpin's physical property and electronic equipment for evidence of violations of "NYS Penal Law and or Federal Statutes," the warrant violated the Fourth Amendment's particularity requirement. See, e.g., United States v. Rosa, 626 F.3d 56, 62 (2d Cir. 2010) (warrant authorizing seizure of electronic equipment without specifying the legal violation "provided [officers] with no guidance as to the type of evidence sought" and constituted a general warrant); United States v. George, 975 F.2d 72, 76 (2d Cir. 1992) ("Mere reference to 'evidence' of . . . general criminal activity provides no readily ascertainable guidelines for the executing officers as to what items to seize . . . . [A]uthorization to search for 'evidence of a crime,' that is to say, any crime, is so broad as to constitute a general warrant."); see also United States v. Burgess, 576 F.3d 1078, 1091 (10th Cir. 2009) ("If the warrant is read to allow a search of all computer records without description or limitation it would not meet the Fourth Amendment's particularity requirement.").

The only crime that is specified in the warrant at issue here is the registration offense. The district court found (and the government concedes) that there was no probable cause to believe that Galpin possessed or produced child pornography – crimes that were mentioned neither in the warrant application nor in the warrant itself, which nonetheless authorized a search for images depicting child sexual activity. While the district court found that the warrant application provided probable cause to believe that Galpin was communicating with and luring young males to his residence, the government does not contend that the warrant authorized officers to search for evidence of luring. Nor could it, given the fact that the warrant neither mentions the luring offense nor incorporated the warrant application. See Groh v.

Ramirez, 540 U.S. 551, 557 (2004) ("The fact that the application adequately described the 'things to be seized' does not save the warrant from its facial invalidity. The Fourth Amendment by its terms requires particularity in the warrant, not in the supporting documents." (emphasis in original)).

While we agree that the warrant was facially overbroad and thus violated the Fourth Amendment, this conclusion does not end the inquiry. As the district court recognized, the proper next steps are, first, to determine whether the warrant is severable – i.e., whether it is possible to carve out the portions of the warrant authorizing a search for evidence of a registration offense from the constitutionally infirm remainder – and, if so, whether the challenged evidence was in plain view when it was seized. Because we find the district court's analysis and the factual record deficient as to both issues, we will vacate the judgment and remand for further proceedings consistent with the discussion that follows.

A. Severability

When a warrant is severable, the portion of the warrant that is "constitutionally infirm . . . – usually for lack of particularity or probable cause – is separated from the remainder and evidence seized pursuant to that portion is suppressed; evidence seized under the valid portion may be admitted." George, 975 F.2d at 79. The severance doctrine is animated by the need to balance the considerable social costs of suppressing evidence of guilt against the need to deter police misconduct, and the judgment that it would be unduly "harsh medicine" to suppress evidence whose seizure was authorized by a particularized portion of a warrant simply because other portions of the warrant failed that requirement. LaFave, Search and Seizure § 4.6(f). However, we have cautioned that severance is not an available remedy for an overbroad warrant "where no part of the warrant is sufficiently particularized, where no portion of the warrant may

be meaningfully severed, or where the sufficiently particularized portions make up only an insignificant or tangential part of the warrant." George, 975 F.2d at 79-80 (internal citations omitted).

We have not previously prescribed how the severance analysis is to be conducted. We do so now, adopting the step-by-step methodology for warrant redaction that was established in United States v. Sells, 463 F.3d 1148 (10th Cir. 2006). First, the court must separate the warrant into its constituent clauses. Id. at 1155; see also United States v. Christine, 687 F.2d 749, 754 (3d Cir. 1982). Second, the court must examine each individual clause to determine whether it is sufficiently particularized and supported by probable cause. Sells, 463 F.3d at 1157. Third, the court must determine whether the valid parts are distinguishable from the non-valid parts. Id. at 1158 ("some part of the warrant must be both constitutionally valid and distinguishable from the invalid portions in order for severability to apply" (quotation marks omitted)); Christine, 687 F.2d at 754 ("Redaction is inappropriate when the valid portions of the warrant may not be meaningfully severable from the warrant as a whole."). To be distinguishable, "each of the categories of items to be seized [must] describe[] distinct subject matter in language not linked to language of other categories, and each valid category [must] retain[] its significance when isolated from rest of the warrant." Sells, 463 F.3d at 1158. In sum, the court must be able to excise from the warrant those clauses that fail the particularity or probable cause requirements in a manner that leaves behind a coherent, constitutionally compliant redacted warrant.

However, the warrant's grammatical amenability to severance is not alone sufficient to justify enforcement of the remainder. The district court must also determine whether the valid portions make up "only an insignificant or tangential part of the warrant."

George, 975 F.2d at 80. Even where parts of the warrant are valid and distinguishable, severance may be inappropriate where, for instance, the sufficiently particularized portion is "only a relatively insignificant part of a sweeping search," United States v. Spilotro, 800 F.2d 959, 967 (9th Cir. 1986), or where "the warrant is generally invalid but as to some tangential item meets the requirement of probable cause," United States v. Freeman, 685 F.2d 942, 952 (5th Cir. 1982); see also United States v. Kow, 58 F.3d 423, 428 (9th Cir. 1995) (severance inapplicable where the constitutionally compliant part is a "relatively insignificant part of an otherwise valid search"). This step of the analysis should not simply be a technical exercise of counting words and phrases but, rather, "a holistic test that examines the qualitative as well as the quantitative aspects of the valid portions of the warrant relative to the invalid portions." Sells, 463 F.3d at 1160.

The district court did not articulate the mode of analysis underlying its conclusion that the warrant was severable. The court appears to have concluded that the warrant could be severed merely by eliminating the authorization to search for (1) evidence of unspecified state or federal offenses and (2) evidence of photographs depicting sexual conduct by a minor. Those two redactions, however, would not cure the warrant's apparent overbreadth. It is important at this juncture to emphasize that the only offense particularized in the warrant was failure to register an internet service provider account or communication identity. The sole legal predicates for a registration offense are possession and usage of an unregistered internet account or communication identifier. The manner or purpose for which the internet account or identifier is used – whether to send an innocuous email, post a picture on MySpace, or to lure minors in a chat room – is not an element of the offense.

Even after the references to state and federal law and images of child pornography are removed, there remain numerous clauses whose relationship to the registration offense is, at best, unclear. After redaction of the two clauses identified above, the first and second paragraphs of the warrant would still broadly authorize a search of "[a]ny computers," "external and internal drives," "digital camera's [sic] and their internal or external storage media," "[a]ny and all computing or data processing software," and any electronic storage device for any evidence substantiating a registration violation, without providing the forensic examiner with any guidance or limitations as to what kinds of files might be relevant. Warrant 1. While those provisions describe the places to be searched, they do not describe with adequate particularity the "items to be seized by their relation to designated crimes." United States v. Williams, 592 F.3d 511, 519 (4th Cir. 2010) (emphasis added). The third paragraph of the warrant particularizes the items that the government may seize, but nothing in the current record explains how the vast majority of those items – e.g., access numbers, passwords, and PINS relating to voice mail systems, computing or data processing literature (including written materials), audio or video cassette tape recordings, books, and magazines – could possibly reveal evidence that Galpin possessed or used an unregistered internet account or communication identity.

Nor did the district court weigh any particularized component(s) of the warrant against the invalid portions to determine whether the particularized portions were insignificant or tangential in relation to the search authorization as a whole. The government asserts that severance was appropriate because "[e]vidence of Galpin's failure to register his online identity . . . was a prominent aspect of the investigation and of the evidence sought to be obtained." However, while the MySpace posting led to probable cause to believe that there was a registration violation, the investigation itself, and the forensic review of Galpin's property,

focused not on his failure to register but on his activities involving young boys and suspected involvement with child pornography. Mere mention of the crime that prompted the investigation will not ensure that an authorization to search for evidence relating to that crime is more than an insignificant or tangential element of a warrant focused on evidence of other criminal activity. See, e.g., Cassady v. Goering, 567 F.3d 628, 636 (10th Cir. 2009). Rather, the court must assess the relative importance on the face of the warrant of the valid and invalid provisions, weigh the body of evidence that could have been seized pursuant to the invalid portions of the warrant against the body of evidence that could properly have been seized pursuant to the clauses that were sufficiently particularized, and consider such other factors as it deems appropriate in reaching a conclusion as to whether the valid portions comprise more than an insignificant or tangential part of the warrant.

Because the current factual record is focused principally on the proper scope and conduct of a computer search for evidence of child pornography and contact with minors, the district court must, on remand, develop a record as to the proper scope and conduct of a search for evidence of the existence of unregistered internet accounts and internet communication identifiers. That record will help to inform the court's determination as to whether any valid portions of the warrant were more than insignificant or tangential and will also be relevant to any plain view and/or good faith determinations that will be necessary if the court determines that the seizures or search exceeded the bounds authorized by any valid aspects of the warrant.

B. Plain View Doctrine

If, on remand, the district court again finds that the warrant was severable but that the evidence of child pornography was outside the properly authorized scope of the search, it will again have to address the question of whether that evidence was in plain view in the course

of the authorized search. The plain view doctrine permits an officer to seize evidence outside a warrant's authorization "when it is immediately apparent that the object is connected with criminal activity, and where such search and seizure do not involve an invasion of privacy." George, 975 F.2d at 78. A quintessential example of a warrantless seizure saved by the plain view doctrine is one by an officer who, acting pursuant to a valid warrant, enters a house to search for a weapon used to commit a crime and seizes a bag of cocaine that he found sitting on the kitchen counter. In order for the search and seizure to not involve an improper invasion of privacy, however, the officer must lawfully have been in the place from which the object could be seen in plain view. Minnesota v. Dickerson, 508 U.S. 366, 375 (1993). Thus, "an essential predicate of the plain view doctrine is that the initial intrusion not violate the Fourth Amendment." George, 975 F.2d at 78; see also Horton v. California, 496 U.S. 128, 136 (1990).

The district court here held that the clause of the warrant authorizing officers to search for evidence of a registration violation permitted the officers to open all of Galpin's computer and digital storage files because opening each file was the only means of determining its content. However if, on remand, the district court finds that the warrant was not severable, then the "initial intrusion" was unconstitutional – the entire hard drive search would have been without valid authorization – and the plain view doctrine could not be invoked to validate the use of any of the evidence the officers seized. The court's determination, on remand, as to the appropriate scope of the authorized search should be informed by a better-developed, more relevant factual record; the court's determination as to whether the image files that were seized would have been in plain view in the conduct of that search will similarly be informed by that augmented record.

Unlike the Ninth Circuit, we have not required specific search protocols or minimization undertakings as basic predicates for upholding digital search warrants, and we do not impose any rigid requirements in that regard at this juncture. See United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1176 (9th Cir. 2010) (en banc) (per curiam). However, the district court's review of the plain view issue should take into account the degree, if any, to which digital search protocols target information outside the scope of the valid portion of the warrant. To the extent such search methods are used, the plain view exception is not available.

As the record is currently constituted, there is little indication as to whether the forensic examiner's search was even directed – much less properly limited – to those files that would substantiate a registration violation. The district court held that the redacted warrant authorized the forensic examiner to open and seize any image file because digital pictures "would be relevant to whether it was actually defendant who was using an unregistered user name or an e-mail account." The district court's speculation as to the probative value of the digital pictures is unsupported by the record developed below and appears somewhat strained, given that officers had determined, before even seeking the warrant, that Galpin's I.P. address was the source of the "Medic Guy" posting and the photograph of Galpin found on the child's MySpace page. The record indicates, moreover, that the investigator opened and played video image files in order to determine whether they contained sexual content. Nothing in the record is indicative of any possible evidentiary connection between the content of video files and the possession of an unregistered internet service provider account, internet communication identifier, or email address. On remand, the district court must determine whether a search limited to evidence of a registration violation would have necessitated the opening of image files

or the playing of video files.[9]

C. Good Faith Exception

The government contends that, even if the warrant was invalid or the pornographic images would not have been in plain view in the course of a properly authorized search, the denial of Galpin's suppression motion should nonetheless be upheld because the investigators reasonably relied on the warrant and the accompanying affidavit when executing the search.

In United States v. Leon, the Supreme Court recognized an exception to the exclusionary rule for "evidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant." 468 U.S. 897, 922 (1984). However, the Supreme Court identified four circumstances in which the good faith exception to the exclusionary rule would not apply:

> (1) where the issuing magistrate has been knowingly misled; (2) where the issuing magistrate wholly abandoned his or her judicial role; (3) where the application is so lacking in indicia of probable cause as to render reliance upon it unreasonable; and (4) where the warrant is so facially deficient that reliance upon it is unreasonable.

United States v. Moore, 968 F.2d 216, 222 (2d Cir. 1992) (citing Leon, 468 U.S. at 923). Because the district court found that the warrant was severable and that the image files had been in plain view, the district court never reached the issue of whether Leon's good faith exception applied to this case.

Galpin argues that the officers deliberately searched for evidence beyond the scope of the probable cause supporting the warrant and thus did not act in good faith. He also

---

[9] Paragraph 3(e) of the warrant authorized a search for "records or correspondence related to the possession, transmission, collection, trading or production of [child pornography]." As explained above, we affirm the district court's uncontested determination that there was no probable cause to search for child pornography.

argues that the warrant application was so lacking in indicia of probable cause, and the face of the warrant was so plainly overbroad, that no officer could reasonably have relied on the warrant when executing the search. The district court's only finding on point was its conditional determination – which the court did not revisit at or after the evidentiary hearing – that the pre-evidentiary hearing record revealed no evidence of deliberate police misconduct. That finding, in any event, only relates to the first of the four circumstances the Leon Court identified as foreclosing the good faith exception.

The district court did not address the question of whether the warrant, which purported to authorize a search for violations of "NYS Penal Law or Federal statutes," was "so facially deficient that reliance upon it [was] unreasonable." See United States v. Moore, 968 F.2d at 222; cf. George, 975 F.2d at 77 (holding that, "[s]ince it was quite clear when [the subject] warrant was executed that 'limits' to a search consisting only of a broad criminal statute were invalid, a fortiori, a warrant not limited in scope to any crime at all is so unconstitutionally broad that no reasonably well-trained police officer could believe otherwise"). Nor has the district court yet had occasion to address the implications for the good faith inquiry of its finding (which we affirm) that the application did not establish probable cause for a search for child pornography.

Here, there is ample evidence that investigators sought evidence beyond the scope of the one crime that was particularized in the warrant application and for which the application supplied probable cause. The forensic examiner testified that, having reviewed a report on the entire investigation, she was looking for images of "younger . . . males," "regardless of whether they're pornographic or not," that she read individual "documents," that she opened and reviewed video files, and that she set up a search filter that identified child pornography websites

Galpin had visited. Indeed, during cross-examination, the examiner confirmed that she went beyond the files that had been identified as potentially indicative of contact with the victims whose names she had been given. Galpin's defense attorney asked: "[A]ssume that [the files identified by targeted searches] comprise[] two percent of all the material that's on the hard drive and the other 98 percent has nothing to do with any of those names . . . . So you look through [the other 98 percent of the files]?" The forensic examiner responded, "[a]bsolutely."

Should the district court determine that neither severability nor the plain view doctrine supports denial of the suppression motion, it will have to determine whether, notwithstanding the exceptions delineated in United States v. Leon, the motion can be denied on the ground that the officers acted in good faith.

CONCLUSION

Accordingly, we AFFIRM the district court's determination that the warrant application failed to establish probable cause to search for evidence of child pornography, and its determination that the warrant's references to the New York State Penal Law and "Federal Statutes" were impermissibly broad. We VACATE the judgment in all other respects and REMAND the case for further proceedings consistent with this opinion.