

allegedly was applying for credit cards online using another individual's identity. *Id.* at 1161. The judge issued the warrant, but was wary about approving such a broad search and imposed a number of restrictions on the search. *Id.* at 1162. The State appealed the search restrictions to the Vermont Supreme Court, arguing that, under the Fourth Amendment, judges must either approve or deny search warrant requests, but may not approve them with conditions. *Id.* at 1163. The court disagreed, holding that conditions limiting the invasiveness of digital searches serve legitimate privacy interests." *Id.* at 1161. The court explained:

A judicial officer might authorize a search of a person, including his pockets, without any particular basis for thinking that evidence will be found in the person's pocket as opposed to elsewhere on his person. But that same officer might permissibly refuse to authorize a search of the person's body cavities based on evidence of similar generality.

Id. at 1171.

The court added:

In short, the warrant application could not have requested a broader authorization: that is, to search all files in all ways on all computers in the house. *See* P. Ohm, Response, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 Va. L.Rev. In Brief 1, 11 (2011) ("Computer search warrants are the closest things to general warrants we have confronted in the history of the Republic."). Understandably, in the judicial officer's view, the warrant application did not provide probable cause for such a wide ranging search. *See United States v. Otero*, 563

F.3d 1127, 1132 (10th Cir. 2009) (“The modern development of the personal computer and its ability to store and intermingle a huge array of one’s personal papers in a single place increases law enforcement’s ability to conduct a wide-ranging search into a person’s private affairs, and accordingly makes the particularity requirement that much more important.”).

Id. at 1175.

Accordingly, the court upheld the following conditions which the judicial officer imposed in an attempt to cure the warrant’s lack of particularity: (1) requiring third parties or specially trained computer personnel to conduct the search behind a “firewall” and provide to State investigatory agents only “digital evidence relating to identity theft offenses”; (2) requiring digital evidence relating to the offenses to be segregated and redacted from surrounding non-evidentiary data before being delivered to the case investigators, “no matter how intermingled it is”; (3) limiting the search protocol to methods designed to uncover only information for which the State had probable cause; (4) precluding the use of specialized “hashing tools” and “similar search tools” without specific authorization of the court; (5) allowing only evidence “relevant to the targeted alleged activities” to be copied to provide to State agents; (6) requiring the State to return “non-responsive data” and to inform the court of this action; (7) directing police to destroy remaining copies of electronic data absent

judicial authorization otherwise; and (8) requiring the State to file a return within the time limit of the warrant to indicate precisely what data was obtained, returned, and destroyed. *Id.* at 1162, 1186. Here, by contrast, the warrant contained no comparable conditions limiting the intrusiveness of the government's search. [R. I, 90-91].

Thus, for all the reasons stated above, the warrant was overbroad. *See, e.g., Horton v. California*, 496 U.S. 128, 140 (1990) ("If the scope of the search exceeds that permitted by the terms of a validly issued warrant or the character of the relevant exception from the warrant requirement, the subsequent seizure is unconstitutional without more."); *In re Grand Jury Subpoena Duces Tecum*, 846 F. Supp. at 12-13 (applying overbreadth doctrine to subpoena, and holding that subpoena for a central processing unit, hard drive, and all computer-accessible data was unconstitutionally overbroad because the hardware contained documents unrelated to the grand jury investigation). As the warrant was overbroad, the trial court erred by denying Knight's Third Motion to Suppress.

D. The invalid portions of the warrant subsume any and all potentially valid portions.

Total suppression of all fruits of the execution of a search warrant is required when "the valid portion of the warrant is 'a relatively insignificant part of an otherwise invalid search.'" *In re Grand Jury Subpoenas*, 926 F.2d at 858 (*quoting*

United States v. Spilotro, 800 F.2d 959, 967 (9th Cir. 1986)). *See also Travers*, 233 F.3d at 1329. In such cases, severance of valid and invalid portions is not an available remedy because, otherwise, “the abuses of a general search would not be prevented.” *United States v. Cardwell*, 680 F.2d 75, 78 (9th Cir. 1982).

Even assuming five (5) out of the twelve (12) items in the warrant were facially valid, total suppression of all fruits of the execution is necessary because the other seven (7) items were facially invalid, the warrant’s valid sections were indistinguishable from the invalid sections, and the warrants invalid parts comprised a greater part of the warrant than its valid parts. *See, e.g., Cassady v. Goering*, 567 F.3d 628, 640 (10th Cir. 2009) (invalidating warrant which contained “one mostly valid and two invalid provisions” after evaluating (1) the number of invalid versus invalid provisions, (2) whether the valid section was sufficiently distinguishable from the invalid sections, and (3) the relative scope and invasiveness of the valid and invalid parts of the warrant).

First, as discussed above, the majority of the warrant was insufficiently particularized and overbroad because it failed to link the items it authorized the government to search and seize to the alleged crime. This factor weighs against the government. *See Cassady*, 567 F.3d at 639 (second and third section of three section warrant invalid because they were not limited by reference to a specific crime).

Second, the warrant's valid sections are indistinguishable from its invalid sections. Item 3 authorized the government to seize and later search:

Computer storage media and the digital content to include but not limited to floppy disks, hard drives, tapes, DVD disks, CD-ROM disks other magnetic, optical or mechanical storage which can be accessed by computers to store or retrieve data or images of child pornography.

[R. I, 90].

But item 1 authorized the government to seize and later search:

Computer hardware to include any and all computer equipment used to collect, analyze, create, display, convert, store, conceal, or transmit electronic magnetic, optical, or similar computer impulses or data. Hardware includes (but is not limited to) any data-processing devices (such as central processing units, personal computers to include "laptop" or "notebook" or "pocket" computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, and other electronic media devices).

[R. I, 90] (emphasis added).

Thus, it is unclear what exactly the warrant permitted the government to do because there is no way to determine whether item 3 limits the scope of item 1 or whether item 1 expands the scope of item 3. The government may only have been authorized to seize internal and peripheral storage devices "which can be accessed by

computers to store or retrieve data or images of child pornography,” as item 3 states, or the government may have been authorized to seize “any and all” internal and peripheral storage devices, as item 1 states. The juxtaposition of items 1 and 12 elicits similar questions. Item 12 authorizes the search and seizure of:

Data maintained on the computer, or computer related storage devices such as floppy diskettes, tape backups, computer printouts, and “zip” drive diskettes, in particular, data in the form of images and/or videos and any accompanying text associated with those images, and/or log files recording the transmission or storage of images, as they relate to violations of Florida law cited herein as related to the possession of distribution of child pornography.

[R. I, 90]. However, much of the “data maintained on the computer, or computer related storage devices” also appears in item 1's unbounded list. It is not apparent which provision trumps the other and, therefore, whether the warrant actually extends to “any and all computer equipment used to collect...data,” as item 1 states. Accordingly, the warrant provides no basis for rationally distinguishing its potentially valid and invalid portions.

Third, the warrant's invalid parts comprise a greater portion than its valid parts. *See Cassidy*, 567 F.3d at 641 (severability is not applicable “if probable cause existed as to only a few of several items listed, or as to a few very particularly described items but not as to other items described in much more general terms”) (internal

quotation marks and citation omitted). The warrant's invalid provisions “allow for the seizure of evidence, whether or not related to [child pornography possession and distribution], and largely subsume those provisions that would have been adequate standing alone.” *See Voss v. Bergsgaard*, 774 F.2d 402, 406 (10th Cir. 1985). The warrant epitomizes a general warrant, and the officers treated it as such. Therefore, the invalid portions of the warrant were sufficiently “broad and invasive” as to “contaminate the whole warrant.” *See Cassady*, 567 F.3d at 641. Accordingly, the trial court erred by denying Knight’s Third Motion to Suppress and the order below should be reversed.

III.

THE SEARCH WARRANT WAS EXECUTED IN AN UNREASONABLE MANNER.

A. Standard of Review

The standard of review on a motion to suppress is a mixed question of fact and law. *Higerd v. State*, 54 So.2d 513, 516 (Fla. 1st DCA 2010). In reviewing a trial court's factual findings, this Court looks to whether competent, substantial evidence supports the trial court's findings. This Court reviews the trial court's application of law *de novo*. *Id.*

B. Unreasonable Execution of Search Warrants

The trial court erred by denying Knight's Fifth Motion to Suppress. All evidence obtained pursuant to the warrant should have been suppressed because the government's execution of the warrant was patently unreasonable. To this day, Knight has been deprived of his electronic equipment and many files that contain no evidence relating to child pornography. Accordingly, the order below denying Knight's Fifth Motion to Suppress should be reversed.

"The general touchstone of reasonableness which governs Fourth Amendment analysis governs the method of execution of the warrant." *United States v. Ramirez*, 523 U.S. 65, 71 (1998) (internal citation omitted). A "seizure lawful at its inception

can nevertheless violate the Fourth Amendment because its manner of execution unreasonably infringes possessory interests protected by the Fourth Amendment's prohibition on 'unreasonable searches.'" *United States v. Jacobsen*, 466 U.S. 109, 124, 104 (1984).

Courts have become increasingly concerned about ensuring that the government's ability to seize entire hard drives for off-site examination does not "become a vehicle" for a plainly unconstitutional "general" search:

We recognize that over-seizing is an inherent part of the electronic search process and proceed on the assumption that, when it comes to seizure of electronic records, this will be far more common than in the days of paper records. This calls for greater vigilance on the part of judicial officers in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures. The process of segregating electronic data that is seizable from that which is not must become a vehicle for the government to gain access to data which it has no probable cause to collect.

United States v. Comprehensive Drug Testing Inc., 621 F.3d 1162, 1177 (9th Cir. 2010).

The "overseizing" that will accompany seizure of a hard drive will often include not only irrelevant material, but also personal non-seizable data.

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. Abdellatif, 2010 WL 5252852 at *5 (W.D.N.Y. 2010).

The dawn of the Information Age has only heightened those [privacy] concerns. The risk of exposing intimate (and innocent) correspondence to prying eyes is magnified because '[c]omputers...often contain significant intermingling of relevant documents with documents that the government has no probable cause to seize.

United States v. Cioffi, 668 F.Supp.2d 385, 391 (E.D.N.Y. 2009).

Here, the State acted unreasonably by retaining numerous items belonging to Knight that agents knew fell outside the scope of the warrant for months after the items were identified. Here, the search warrant was executed on September 9, 2009, yet Boymer did not complete his forensic examination of the computer until March 20, 2010, over six months after the computer was seized. [R. I, 145]. Moreover, Knight was not arrested until April 19, 2010 pursuant to a warrant obtained based upon the examination of the computer. [R. I, 146]. Yet the State failed to make any effort to return Knight's non-contraband personal effects to Knight after completing its forensic analysis and associated police report.

In *United States v. Mitchell*, 565 F.3d 1347, 1351 (11th Cir. 2009), the court held that the defendant's motion to suppress should have been granted because there

was “no compelling justification for the [government's twenty-one day] delay” in obtaining a search warrant for the defendant's seized hard drive. Thus, the mere possibility that the defendant's hard drive could be free of evidence relating to child pornography combined with the government's delay in taking steps to return non-incriminating property, *i.e.*, obtain a warrant authorizing a search, was sufficient to warrant suppression of the seized evidence. *Id.* at 1352 (“the sooner the warrant issues, the sooner the property owner’s possessory rights can be restored if the search reveals nothing incriminating”) (internal citation and quotation marks omitted). But here, agents knew as of March 20, 2010, that many files and electronic documents of Knight’s contained no evidence relating to his alleged criminal activity. [R. I, 146]. Yet, those items remain unreturned to Knight. *Id.*

While some of Knight’s seized property contained alleged contraband, there is “no doubt” that Knight retained “significant possessory interest[s]” in his seized equipment. *See United States v. Laist*, 702 F.3d 608, 616 (11th Cir. 2012). In *Laist*, the defendant was afforded an opportunity to remove “whatever he wanted to download” before agents seized his computer and hard drives, and he removed files he needed for school. *Id.* at 611. Nonetheless, the court held that, “[s]ince the possessory interest in a computer derives from its highly personal contents, the fact that Laist had a real opportunity to copy or remove personal documents reduces the

significance of his interest.” *Id.* (emphasis added). Thus, even the opportunity to copy personal non-contraband files – an opportunity Knight was never given-did not extinguish *Laist*’s possessory interest in his seized computer and hard drives. *Id.*

Moreover, “[i]t is the government’s duty to comply with the Fourth Amendment.” *Jacobsen*, 466 U.S. at 113. *See also Mitchell*, 565 F.3d at 1352 (general rule that the government should swiftly return non-incriminating evidence applies with “even greater force to the hard drive of a computer, which is the digital equivalent of its owner’s home, capable of holding a universe of private information.”); *United States v. Delancy*, 502 F.3d 1297, 1308 (11th Cir. 2007) (A consent to search may be insufficient where the consent itself springs from prior illegal activity by the police, such as an unlawful entry. Knight’s efforts to reacquire his lawfully owned property are therefore irrelevant.

Well-established Fourth Amendment principles further support Knight’s claim that the government unreasonably executed the warrant. A “‘seizure’ of property occurs when there is some meaningful interference with an individual’s possessory interests in that property.” *Jacobsen*, 466 U.S. at 113. Even where one no longer holds a privacy interest in seized property, he may hold a possessory interest that continues to survive long after the seizure takes place. *See United States v. Paige*, 136 F.3d 1012, 1021-22 (5th Cir. 1998). Moreover, a seizure of property may begin

as reasonable but then ripen into a seizure that violates the Fourth Amendment. *United States v. Place*, 462 U.S. 696, 710 (1983) (although warrantless detention of a traveler's luggage did not initially violate the Fourth Amendment, the retention of that luggage for over ninety (90) minutes rendered the seizure unreasonable and violated the Fourth Amendment). Therefore, whenever the government meaningfully interferes with an individual's interest in property, a "seizure" subject to the reasonableness analysis of the Fourth Amendment takes place.

The Supreme Court's recent Fourth Amendment jurisprudence shows that property rights are a paramount concern. "The Amendment establishes a simple baseline, one that for much of our history formed the exclusive basis for its protections. When the Government obtains information by physically intruding on persons, houses, papers, or effects, a search within the original meaning of the Fourth Amendment has undoubtedly occurred. *Florida v. Jardines*, 133 S. Ct. 1409, 1414 (2013) (internal quotation marks omitted). Thus, "[a]t bottom, [courts] must assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.... For most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates." *United States v. Jones*, 132 S. Ct. 945, 950 (2012) (government's installation of a GPS device on a target's

vehicle, and its use of that device to monitor the vehicle's movements, constitutes a "search" because the government physically occupied private property for the purpose of obtaining information) (internal quotation marks and citations omitted).

Additionally, in the civil context, courts have recognized that constitutional violations can occur when the government acts with unreasonable delay in returning property, which initially was lawfully seized. *Lathon v. City of St. Louis*, 242 F.3d 841 (8th Cir. 2001) (holding that ammunition and weapons seized from resident's possession pursuant to valid search warrant did not preclude resident's Section 1983 claim that government's subsequent refusal to return ammunition and weapons constituted deprivation of property without due process; pivotal deprivation was not initial seizure of items, but the refusal to return them without court order after it was determined that items were not contraband or required as evidence in court proceeding); *see also Presley v. City Of Charlottesville*, 464 F.3d 480 (4th Cir. 2006) (In order for property owner to state a claim against city under § 1983 for unreasonable seizure of real property in violation of Fourth Amendment, based on city's publishing a map showing a public trail crossing owner's property and encouraging private individuals to trespass on the property, property owner did not have to allege that she was completely deprived of her possessory interests in her property; owner had only to allege that there was some meaningful interference with

her possessory interests in the property). Similarly, for many years, courts have determined the reasonableness of the government's continued possession of private property in the adjudication of Rule 41(e) motions as civil equitable actions for the return of property. *See, e.g., Soviero v. United States*, 967 F.2d 791, 792-93 (2d Cir. 1992); *Mora v. United States*, 955 F.2d 156, 158 (2d Cir. 1992); *United States v. Martinson*, 809 F.2d 1364, 1368 (9th Cir. 1987); *Sovereign News Co. v. United States*, 690 F.2d 569, 577 (6th Cir. 1982).

Therefore, it is unremarkable for Knight to claim that the government's prolonged retention of his property was unreasonable. What is remarkable, however, is the government's disregard of Knight's property rights to his computer equipment and files not subject to forfeiture that contained a "universe of information." *Mitchell*, 565 F.3d at 1352. It is undeniable that the State meaningfully interfered with Knight's possessory interest in his seized property. Additionally, the State has not offered a reasonable explanation for its continued failure to even attempt to return any of Knight's property that agents had completed analyzing and knew was contraband-free. Accordingly, the search warrant for Knight's property was executed in an unreasonable manner and the trial court erred by denying Knight's Fifth Motion to Suppress.

CONCLUSION

For all of the foregoing reasons, the orders below denying Knight's second, third and fifth motions to suppress should be reversed.

Respectfully submitted,



Wm. J. Sheppard, Esquire
Florida Bar No.: 109154
Elizabeth L. White, Esquire
Florida Bar No.: 314560
Matthew R. Kachergus, Esquire
Florida Bar No.: 503282
Bryan E. DeMaggio, Esquire
Florida Bar No.: 055712
Sheppard, White & Kachergus, P.A.
215 Washington Street
Jacksonville, Florida 32202
Telephone: (904) 356-9661
Facsimile: (904) 356-9667
COUNSEL FOR APPELLANT

CERTIFICATE OF SERVICE


I HEREBY CERTIFY that a copy of the foregoing has been furnished to **Trisha Meggs-Pate, Esquire**, Assistant Attorney General, The Capitol, Suite PL-01 Tallahassee, Florida 32399, by Electronic Mail, this 18th day of December, 2013.



ATTORNEY

CERTIFICATE OF COMPLIANCE

Undersigned counsel certifies that the size and style of type used in this brief is 14 point Times Roman.



ATTORNEY

ldh[knight.john.initial.brief]