IN THE DISTRICT COURT OF APPEAL
OF FLORIDA
FIRST DISTRICT

APPEAL DOCKET NO.: 1D13-3182

JOHN GORDON KNIGHT,

Appellant,

vs.

STATE OF FLORIDA,

Appellee.

On Appeal from the Circuit Court, Fourth Judicial Circuit, in and for Duval County, Florida

---

REPLY BRIEF OF APPELLANT

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 & DeMaggio, P.A.
215 Washington Street
Jacksonville, Florida 32202
Telephone: (904) 356-9661
COUNSEL FOR APPELLANT

TABLE OF CONTENTS

Page

TABLE OF CONTENTS ..... *i*

TABLE OF CITATIONS ..... *iii*

ARGUMENT 1

I.

THE INVESTIGATION OF KNIGHT'S COMPUTER AND KNIGHT'S ARREST WERE THE PRODUCT OF AN ILLEGAL EXTRA-JURISDICTIONAL INVESTIGATION 1

A. Knight Had Standing to Contest the Extra-Jurisdictional Investigation of Him 1

B. Police Conducted an Illegal Extra-Jurisdictional Investigation of Knight's Computer 3

C. The Good Faith Exception Does Not Apply 5

TABLE OF CONTENTS (Continued)

Page

II.

THE WARRANT AUTHORIZING THE SEARCH OF KNIGHT'S COMPUTER WAS FACIALLY INVALID BECAUSE IT LACKED PARTICULARITY AND WAS OVERBROAD 7

A. Knight's Third Motion to Suppress Properly Preserved the Issues of Lack of Particularity and Over Breadth 7

B. The Search Warrant Constituted an Unreasonable Search and Seizure Because it Failed the Fourth Amendment's Particularity Requirement 8

C. The Good Faith Exception Does Not Apply 14

III.

THE SEARCH WARRANT WAS EXECUTED IN AN UNREASONABLE MANNER 17

CONCLUSION 22

CERTIFICATE OF SERVICE 23

CERTIFICATE OF COMPLIANCE 24

TABLE OF CITATIONS

Case(s) **Page**

In re Applications for Search Warrants for Information Associated with Target Email Accounts/Skype Accounts, 2013 WL 4647554 (D.Kan. 2013) 10-11

In re Matter of Black iPhone 4., 2014 WL 1045812 (D. D.C. 2014) 11

In re Search of Information Associated with [redacted] @mac.com That is Stored at Premises Controlled by Apple, Inc., 2014 WL 945563 (D. D.C. 2014) 12

In re Search Information Associated with the Facebook Account Identified by the Username Aaron Alexis That is Stored at Premises Controlled by Facebook, Inc., 2013 WL 7856600 (D. D.C. 2013) 12

In re Search of 3817 W.West End, First Floor Chicago Illinois 60621, 321 F.Supp.2d 953 (N.D. Ill. 2004) 10

Lo-Ji Sales, Inc. v. New York, 442 U.S. 319 (1979) 14

Oleandi v. State, 731 So.2d 5 (Fla. 4th DCA 1999) 19

Parker v. State, 362 So.2d 1033 (Fla. 1st DCA 1978) 4-5

TABLE OF CITATIONS (Continued)

Case(s) **Page**

Rokas v. Illinois,
439 U.S. 128 (1978) 1,2

State v. Allen,
790 So.2d 1122 (Fla. 2d DCA 2001) 4,5

State v. Chapman,
376 So.2d 262 (Fla. 2d DCA 1979) 4

State v. Sills,
852 So.2d 390 (Fla. 4th DCA 2003) 2

T.T.N. v. State,
40 So.3d 897 (Fla. 2d DCA 2010) 5

U.S. v. Comprehensive Drug Testing, Inc.,
513 F.3d 1085 (9th Cir. 2008) 9

United States v. Cioffi,
668 F.Supp.2d 385 (E.D. N.Y. 2009) 14-15

United States v. Ganias,
2014 WL 2722618 (2d Cir. 2014) 17-18,20

United States v. George,
975 F.2d 72 (2d Cir. 1992) 15

United States v. Leon,
468 U.S. 897 (1984) 5-6,14,16

TABLE OF CITATIONS (Continued)

Case(s) **Page**

United States v. Tamura,
694 F.2d 591 (9th Cir. 1982) 11-12,19

United States v. Upham,
168 F.3d 532 (1st Cir. 1999) 8-9

Wilson v. State,
403 So.2d 982 (Fla. 1st DCA 1978) 4,5

Statutes and Rules

§23.1225, Fla. Stat. (2013) 6

§901.25, Fla. Stat. (2013) 6

§923.1051 (2013) 7

ARGUMENT

I.

THE INVESTIGATION OF KNIGHT'S COMPUTER AND KNIGHT'S ARREST WERE THE PRODUCT OF AN ILLEGAL EXTRA-JURISDICTIONAL INVESTIGATION.

A. Knight Had Standing to Contest the Extra-Jurisdictional Investigation of Him

Knight's motion to suppress is not barred by Fourth Amendment cases that require a reasonable expectation of privacy to support a motion to suppress because the motion contested an extra-jurisdictional investigation in violation of state law rather than a Fourth Amendment violation. In order to sustain the extra-jurisdictional investigation, the State improperly relies on *Rakas v. Illinois*, 439 U.S. 128, 130 n. 1 (1978) for the proposition that a defendant must prove that his Fourth Amendment rights were violated by the challenged search or seizure in order to have standing to bring *any* motion to suppress. [Answer Brief 13–15].

However, *Rakas* specifically held that a defendant had the burden of proving a violation of Fourth Amendment rights in order to bring a motion to suppress the fruits of the *search and seizure* of an automobile and rifle that the defendant did not own. 439 U.S. at 129. In that case, the only grounds that the defendant could rely on in his motion to suppress was an unreasonable search and seizure. Knight's second motion to suppress, by contrast, contested the State's illegal *investigation* of his

activity rather than a search and seizure. Applying the *Rakas* holding to the instant case would be nonsensical, since it would essentially require the defendant to prove that he was the victim of an unlawful search and seizure when the conduct the motion complains of is not a search and seizure.

While the instant case and many of the cases that Knight relies upon, involve searches and seizures, the prohibition on extra-jurisdictional investigations encompasses not just searches and seizures, but also activity that normally would not qualify for Fourth Amendment protections. For example, *State v. Sills*, 852 So.2d 390, 392 (Fla. 4th DCA 2003) specifically involved the issue of whether officers had obtained the defendant's consent to search his home outside their jurisdiction. While the motion to suppress targeted the fruits of a police search, the illegal conduct complained of included acts such as transporting the defendant in handcuffs outside their jurisdiction and executing a waiver allowing them to search his home bearing the crest of a different police department. *Id.* at 393. Even though the illegal conduct that the defendant in *Sills* complained of culminated in a search, the court suppressed the evidence because of the extra-jurisdictional investigation itself, which involved activity that did not constitute a search. *Id.*

Because the extra-jurisdictional investigation doctrine is a ground to suppress evidence under state law, rather than federal law, Knight does not need to show that

he had a reasonable expectation of privacy for his activity on the peer-to-peer network. Rather, Knight's Second Motion to Suppress was predicated on the illegal *investigation*, which included activity falling beyond the scope of Fourth Amendment protection. For this reason, the State's arguments that Knight did not have standing to bring a motion to suppress are unpersuasive.

B. Police Conducted an Illegal Extra-Jurisdictional Investigation of Knight's Computer.

The State has also failed to rebut Knight's argument that Detective Burban engaged in an extra-jurisdictional investigation. Its primary contention is that the investigation occurred within Burban's jurisdiction because the files she investigated were located in a folder that was accessible to the public. This argument is unconvincing for two reasons. First, Burban's investigation extended beyond simply viewing the files in Knight's shared folder. Second, under Florida law, even investigations that take place in public locations may constitute an illegal extra-jurisdictional search.

The State focuses solely on Burban's inspection of Knight's shared folder and ignores the fact that she performed a full-scale investigation of Knight's computer and home, which included locating his home address, obtaining a search warrant, travelling to his home, and performing a search of his computer. [R. I. 5, 89–91; R.

III 427–431]. Even assuming that Burban was not investigating Knight by monitoring his online activity, these other acts, even standing alone, constituted an illegal extra-jurisdictional investigation. In both *State v. Allen*, 790 So.2d 1122 (Fla. 2d DCA 2001) and *Wilson v. State*, 403 So.2d 982 (Fla. 1st DCA 1978), the courts found that seeking an arrest warrant for property outside of a police officer's jurisdiction is an extra-jurisdictional investigation under color of office that cannot be saved absent a Mutual Aid Agreement. Furthermore, the presence of other officers during Burban's search of Knight's home did not cure the illegality of the extra-jurisdictional search. *Allen*, 790 So.2d at 1122 (finding that detective's extra-jurisdictional search was unlawful where the search occurred in the presence of a deputy sheriff in that jurisdiction).

Moreover, simply because Knight's online activity was accessible to the public, does not mean that a police officer from another jurisdiction may investigate that activity. The State's argument once again relies on the faulty premise that the extra-jurisdictional investigation doctrine is rooted in Fourth Amendment privacy concerns rather than state law limitations on the authority of municipal officers. Extra-jurisdictional investigations by municipal police officers are limited to those instances where the subject matter of the investigation originate inside the city limits. *State v. Chapman*, 376 So.2d 262 (Fla. 2d DCA 1979); *Parker v. State*, 362 So.2d 1033 (Fla.

1st DCA 1978). Just because an officer observes public activity that arouses suspicion, even if they observe that activity from within their jurisdiction, does not permit them to engage in an investigation of subject matter originating from outside their jurisdiction. *See T.T.N. v. State*, 40 So.3d 897, 898 (Fla. 2d DCA 2010) (finding that officer performed an extra-jurisdictional investigation where officer observed a driver flee from a traffic stop in public and within his jurisdiction, but proceeded to the driver's home, located outside his jurisdiction, where he discovered drugs).

Furthermore, the State's attempts to distinguish the instant case from *Wilson* and *Allen* by pointing out that Burban was physically located within her jurisdiction when she performed the investigation are unconvincing. The standard for extra-jurisdictional investigations focuses on where the *subject matter* of the investigation originates, rather than the officer's physical location during the same. Here, the doctrine would be effectively nullified if this Court were to accept the State's argument as law enforcement could investigate any crime *anywhere* via the internet as long as they remained physically stationed at a computer in within their jurisdiction.

C. The Good Faith Exception Does Not Apply

The *Leon* good faith exception does not apply to this case because the exception only applies to Fourth Amendment challenges, and because Burban did not

carry out her investigation in good faith. *United States v. Leon*, 468 U.S. 897 (1984) dealt specifically with an exception to the Fourth Amendment exclusionary rule, and none of the cases cited by the State deal with extra-jurisdictional investigations. Furthermore, none of the cases Knight relies on in asserting his argument contemplate applying the good faith exception to extra-jurisdictional searches.

Even if the court adopted a good-faith exception to extra-jurisdictional investigations, Burban did not act in good faith by investigating Knight's personal computer. The concept of municipal officer jurisdiction is well-entrenched in Florida law. *See*, *e.g.*, § 23.1225, Fla. Stat. (2013) (establishing exception to municipal jurisdiction for mutual aid agreements); § 901.25, Fla. Stat. (2013) (establishing "fresh pursuit" exception for extra-jurisdictional arrests). Given these statutes, it would be entirely unreasonable to conclude that Burban would be allowed to carry out an extra-jurisdictional investigation.

II.

THE WARRANT AUTHORIZING THE SEARCH OF KNIGHT'S COMPUTER WAS FACIALLY INVALID BECAUSE IT LACKED PARTICULARITY AND WAS OVERBROAD.

A. Knight's Third Motion to Suppress Properly Preserved the Issues of Lack of Particularity and Over Breadth.

The State argues that Knight did not preserve the particularity issue on appeal because he did not raise an objection sufficient to put the trial court on notice of the error. [Answer Brief, 24–25]. An objection is preserved if it is "sufficiently precise that it fairly apprised the trial court of the relief sought and the grounds therefore". § 923.051(3), Fla. Stat. (2013). Knight's Third Motion to Suppress clearly stated that the search warrant was defective on the grounds that it failed to meet the particularity requirement of the Fourth Amendment. [R. I, 75–6]. This is the exact issue that Knight now raises on appeal. The broad scope of the warrant and the lack of reference to a particular crime are both causes of the warrant's unreasonable authorization of a general search, but the underlying ground for appeal is the general search itself. Therefore, all issues raised in Knight's initial brief were properly preserved on appeal.

B. The Search Warrant Constituted an Unreasonable Search and Seizure Because it Failed the Fourth Amendment's Particularity Requirement.

The search warrant fails to meet the Fourth Amendment's particularity requirement because it allowed the police to perform a general search of all files on Knight's computer, without limitation by reference to the crime the defendant was suspected of. The State contends that the warrant is facially valid in that it specified the place to be search and the items to be seized by providing a description of the Knight's residence and computer equipment. [Answer Brief, 29]. The State relies primarily on *United States v. Upham*, 168 F. 3d 532 (1st Cir. 1999) to support its argument that a warrant authorizing the seizure of an entire computer and all files thereon meets the Fourth Amendment's particularity requirement. [Answer Brief, 28, 30–31]. While the *Upham* court did conclude that a warrant which authorized the search and seizure of the defendant's computer equipment was constitutional, its holding rested on the assumption that "the seizure and subsequent off-premises search of the computer . . . was the narrowest definable search and seizure likely to obtain the images" and "if the images themselves could have been easily obtained through an on-site inspection, there might have been no justification for allowing the seizure of *all* computer equipment." *Id.* at 535.

The *Upham* court likely ruled as it did because computer-search technology was more limited in 1999, when *Upham* was decided, or because the defendant in that case failed to argue alternatives to an unfettered search on appeal. However, the notion that an unfettered search of an entire computer is the narrowest search procedure available to law enforcement (the proposition on which both *Upham* and the State's arguments rely) is far from true in the second decade of the twenty-first century.

Other Circuits have specified methods for police officers to narrow their pre-search criteria for electronic searches in order to avoid violating the Fourth Amendment's particularity requirement. Most notably, in *U.S. v. Comprehensive Drug Testing, Inc.*, 513 F.3d 1085 (9th Cir. 2008), the court promulgated five pre-search guidelines for narrowing searches of digital information. Two of those guidelines are particularly relevant to the present issue: (1) the government must design a search protocol to uncover only the information for which it has probable cause and (2) the segregation and redaction of data not covered by probable cause must be sorted by an independent third party or government computer personnel who do not disclose the segregated data to the investigators. *Id.* at 1180.

A blanket warrant to search the entire contents of a digital device fails to meet the particularity requirement absent a search protocol that limits the methods police

may use to search the device. *In re Search of 3817 W. West End, First Floor Chicago, Illinois 60621*, 321 F. Supp. 2d 953, 957 (N.D. Ill. 2004) ("What the government seeks is a license to roam through everything in the computer without limitation and without standards. Such a request fails to satisfy the particularity requirement of the Fourth Amendment . . . .") (hereinafter *West End*). Courts often find search protocols are a necessary constitutional prerequisite for computer searches because the search of a computer presents heightened particularity concerns not found in warrants for searches of tangible objects, such as files in a file cabinet. Such factors include: (1) given the difficulty of on-site searches, police officers often have to seize a large number of files before searching them; (2) digital searches present a substantial likelihood that the computer contains intermingling of files the police have probable cause to search with files the police do not have probable cause to search; (3) computers are capable of storing an extraordinary volume of data; and (4) computers present enhanced tools to refine file searches instantly. *Id.* at 958–959.

Given the substantial particularity concerns that digital searches present, magistrate judges often deny warrants for digital searches that lack adequate search protocols. *See, e.g.*, *Id.* at 957 (requiring search protocol for warrant authorizing the search of an entire computer); *In Re Applications for Search Warrants for Information Associated with Target Email Accounts/Skype Accounts*, 2013 WL

4647554, *4–*6 (D. Kan. 2013) (holding that warrant for carte blanche search of two of suspect's e-mail accounts violated the Fourth Amendment's particularity requirement); *In Re Matter of Black iPhone 4,* , ---F. Supp. 2d ---; 2014 WL 1045812, *4–*5 (D. D.C. 2014) (requiring search protocol for warrant authorizing search of suspects' phones and computers to comply with the Fourth Amendment's particularity requirement). While these rulings do not lay down rigid guidelines for search protocols, at a minimum, such protocols should indicate whether an entire device will be imaged, how long the images will be stored, and what procedures will be used to avoid viewing material that is not supported by the warrant. *Id.* at *4.

Given the fact that searches of computer data present a heightened danger of co-mingling data that is and is not supported by probable cause, courts often require police officers to enact independent information filtration procedures to ensure that the investigators are not exposed to information that the Fourth Amendment prohibits them from searching. A pre-digital example of this phenomenon can be found in *United States v. Tamura*, 694 F.2d 591, 595–596 (9th Cir. 1982) where the court held that the wholesale search and seizure of eleven cardboard boxes violated the Fourth Amendment's particularity requirement, when the documents which the police had probable cause to obtain were comingled with files that they lacked probable cause to obtain. The court held that in some cases, wholesale search and seizure would be

permissible, but that in those cases, the government would be required to enact an "essential safeguard" that the search be monitored by a neutral, detached magistrate. *Id.*

The concerns raised in *Tamura* about searches of comingled data apply with greater force in the context of digital searches. Data involving illicit activity are more likely to be comingled with files unrelated to the illicit activity on a digital storage device. *See, e.g. In Re Search Information Associated with the Facebook Account Identified By the Username Aaron. Alexis That is Stored at Premises Controlled by Facebook, Inc.*, 2013 WL 7856600, ---F. Supp. 2d --- (D. D.C. 2013) (holding that police could seize all information on suspect's Facebook account and segregate data that they had probable cause to obtain only if they implemented an independent screening procedure for separating the comingled data); *In Re Matter of Search of Information Associated with [redacted] @mac.com that is Stored at Premises Controlled by Apple, Inc.*, --- F. Supp. 2d ---; 2014 WL 945563 (D. D.C. 2014) (holding that government could not search all of the correspondence in the suspect's e-mail account, but instead was required to let the service provider screen the e-mails according to search criteria specified by the government.) (hereinafter *in re search of mac.com*)

The search warrant in the instant case provides none of the particularity safeguards recommended by the emerging body of law on digital searches. Instead, paragraph three of the government's search warrant allows the seizure and off-site searches of all Knight's computer storage media that "can be accessed by computers to store or retrieve data or images of child pornography" [R. I, 90–91]. By definition, any computer storage medium owned by Knight could potentially be used to store or retrieve child pornography, so the warrant effectively allows the kind of wholesale search and seizure of an entire computer that the authorities cited above decry for lacking particularity.

The fact-specific nature of the particularity inquiry means there are few bright-line rules for digital searches. However, neither the search warrant nor the State's arguments have offered a justification for why the investigation would have been prejudiced by a sensible limitation on the warrant's scope, like limiting the search of Knight's computer to certain key words, using hashing tools to look up or compare data, use of forensic software like EnCase, or limiting searches only to certain types of files. Additionally, the State did not offer a process for segregating comingled data or provide a justification for why it would be reasonable for the investigators to sort through Knight's comingled data themselves. For these reasons, an unfettered search of Knight's computer without a screening procedure or search protocol violated

Knight's constitutional rights by failing to meet the Fourth Amendment's particularity requirement.

C. The Good Faith Exception Does Not Apply

The good faith exception to the exclusionary rule does not apply in this case because the search warrant was objectively unreasonable. The State argues that even if the search warrant violated the particularity requirement, the fruits of the unconstitutional search should not be excluded under *Leon* because the government relied on the probable cause determination of a warrant issued by a magistrate. However, *Leon* holds that for the good faith exception to apply, the officer's reliance on the magistrate's probable-cause determination, and on the technical sufficiency of the warrant, must be objectively reasonable. *Id.* at 922. Additionally, the exception does not apply where the issuing magistrate has "wholly abandoned his judicial role" by issuing a generalized search warrant. *Id.* (citing *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319 (1979)).

In the context of digital searches, authorizing an unrestricted search of a suspect's computer is objectively unreasonable. In *United States v. Cioffi,* 668 F. Supp. 2d 385, 388 & 396 (E.D.N.Y. 2009), the court held that a search warrant authorizing the search and seizure of all e-mails sent and received on the suspect's e-mail account within a one month period was unconstitutional. The government

argued that even though the warrant was unconstitutionally broad, the *Leon* good faith exception applied because the Second Circuit had not established clear rules on how to conduct digital searches in a particularized manner. *Id.* at 397. The court held that because the issue with the warrant did not involve the specifics of the search protocol, but instead implicated the "fundamental and venerable prohibition on general search warrants" by allowing an unrestricted search of the defendant's e-mail messages without reference to the particular crime or criminal activity to which the crime must relate, no officer with reasonable training would have relied on the warrant. *Id.* at 397 (quoting *United States v. George*, 975 F. 2d 72, 77 (2d Cir. 1992)).

Like the warrant at issue in *Cioffi*, the warrant in the instant case allowed a broad search of Knight's personal information, without reference to any crimes Knight was suspected of. Furthermore, the warrant in this case authorized a far more expansive search of Knight's belongings because it allowed search of the Knight's entire computer, rather than just the e-mails Knight sent and received during a one month period. Even if it would be reasonable for the police officers not to understand the constitutional nuances of search protocols and screening procedures, surely it would defy reason for a police officer to believe that he had probable cause to access every single file on Knight's computer while searching for a limited number of pictures and videos. Any person with a lay understanding of privacy and computer

technology, much less an officer specifically trained to perform police investigations, would be aware that Knight's computer contained personal files like e-mail correspondence, family photos, and other personal documents, which a police investigation into possession of child pornography has no right to reach. Accordingly, the *Leon* good faith exception to the exclusionary rule does not apply.

III.

THE INVESTIGATORS EXECUTED THE SEARCH WARRANT IN AN UNREASONABLE MANNER.

The search warrant was executed in an unreasonable manner because the police unreasonably seized Knight's personal possessions and held them for six months. The State offers two rationales for the prolonged seizure: first, that the difficulty of performing computer searches made the seizure necessary and, second, that it needed to keep the computer because it did not know which files would be used as evidence at the time Knight filed his Fifth Motion to Suppress. [Answer Brief, 36–37]. Neither of these justifications address Knight's two primary concerns on this issue: (1) that the police deprived Knight access to personal files unrelated to the child pornography investigation and (2) Knight was deprived of his computer hardware, which the police did not require to conduct their investigation.

A search warrant is executed unreasonably when the State retains all of the defendant's electronic files for an unreasonable period of time without returning or purging the files that are unrelated to their search. *United States v. Ganias*, ---F.3d---; 2014 WL 2722618, *10 (2d Cir. 2014). In *Ganias*, Army investigators obtained a warrant to perform a search of the defendant's computer files for evidence of theft and fraud carried out by his accounting company. *Id.* at *1. Army investigators seized

the defendant's files by copying forensic mirror images of his entire computer while they searched his home. *Id.* The government then retained those files for two-and-a half years, and later used files which were non-responsive to the original warrant to execute a new warrant for his files of unrelated crimes of tax fraud. *Id.* at *2–*3. The Second Circuit held that the search warrant had been executed unreasonably because the government's retention of the copies of the defendant's personal files for two-and-a-half years deprived him of exclusive control of his property for an unreasonable amount of time. *Id.* at *10.

The court recognized that the creation of mirror images of a defendant's hard drive was constitutionally permissible because such images allow investigators to search the defendant's computer as if they were searching his actual hard drive, without interfering with the defendant's use of his files. However, it also held that such searches and retention of files were still subject to Fourth Amendment reasonableness requirements. *Id.* at *8. The court rejected the government's arguments that the retention of files was necessary to conduct the investigation and authenticate the evidence at trial, holding that such justifications were insufficient to justify the defendant's loss of exclusive control over the files. *Id.* at *10–*12.

Other circuits have also held that when data which is pertinent to an investigation are comingled with data that the police do not have probable cause to

obtain the police must establish a procedure to return or destroy the data which they lack the authority to possess. In *Tamura*, the court found that the government's wholesale search and seizure of the defendant's boxes of files violated the constitution because the government refused to return unrelated items to the defendant. *Tamura*, 694 F.2d at 596. These concerns are particularly acute in the digital context where the government can seize massive amounts of data and destroy or return irrelevant data with relative ease. *See*, *in re mac.com*, 2014 WL 9455673, *6 (requiring the government to destroy all contents and records that are not within the scope of the investigation as outlined in the search warrant).

Furthermore, the State's arguments regarding the uncertainty of which files would be entered into evidence ring false because an investigation of the contents of a computer's hard drive does not require a prolonged seizure of the suspect's entire computer. To justify the state's six month seizure of the defendant's computer hardware the State cites *Oleandi v. State*, 731 So. 2d 5 (Fla. 4th DCA 1999) for the proposition that courts possess the inherent right to refuse to return a criminal defendant's property. However, *Oleandi* dealt with the seizure of physical goods that were stored in a warehouse where the defendant stored stolen property. *Id.* In that case, any of the physical goods in the warehouse could have been necessary for the State to present its case. In the context of digital searches, however, data can easily

be copied, shared, and analyzed without disturbing the defendant's dominion and control of the hardware that originally stored that data.

The instant case presents identical constitutional deficiencies in the execution of the warrant as those outlined by *Ganias* and similar cases. As in *Ganias*, the State held Knight's computer for an unreasonably long period of time without making an effort to return or delete the files that where unresponsive to the warrant. [R. I, 5]. Furthermore, the State's execution of the warrant was far more egregious here than in *Ganias* because not only did the State deprive Knight of exclusive dominion and control of his files, but deprived him of total dominion and control by seizing his entire computer rather than making a mirror image of the hard drive.

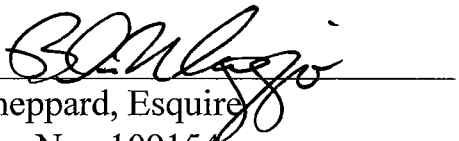
Additionally, the State failed to assert any justification for why Knight was deprived access to both his computer hardware and personal files. The State simply did not require any of these items to carry out its investigation or present its case. Any files that were required could have been copied from Knight's hard drive without interfering with Knight's possessory rights to his computer. The State did not require Knight's original hard drive, his processor, his motherboard, or any of the other computer components they seized to conduct its investigation. The six-month seizure of Knight's entire computer only served to deprive him of his belongings, and did not aid its investigation in any way. For these reasons, the State unreasonably executed

the search warrant, and the trial court erred in denying Knight's Fifth Motion to Suppress.

CONCLUSION

For all the reasons set forth herein, this Court should reverse Knight's conviction.

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 & DeMaggio, P.A.
215 Washington Street
Jacksonville, Florida 32202
Telephone: (904) 356-9661
Facsimile: (904) 356-9667
COUNSEL FOR APPELLANT

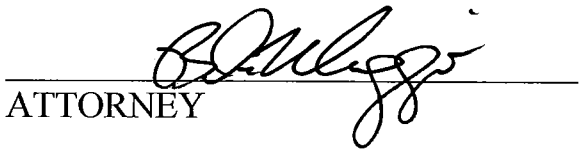
CERTIFICATE OF SERVICE

I HEREBY CERTIFY that a copy of the foregoing has been furnished to **Wesley Cross Paxson, Esquire,** Assistant Attorney General, The Capitol, Suite PL-01, Tallahassee, Florida 32399-1050, by Electronic Mail, this 30th day of June, 2014.

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.reply.brief]