

IN THE DISTRICT COURT OF APPEAL OF FLORIDA
SECOND DISTRICT

RECEIVED, 11/19/2015 12:53:29 PM, Clerk, Second District Court of Appeal

STATE OF FLORIDA,	:	
	:	
Appellant,	:	
	:	
vs.	:	Case No. 2D14-4283
	:	
AARON STAHL,	:	
	:	
Appellee.	:	
_____	:	

APPEAL FROM THE CIRCUIT COURT
IN AND FOR SARASOTA COUNTY
STATE OF FLORIDA

ANSWER BRIEF OF APPELLEE

HOWARD L. "REX" DIMMIG, II
PUBLIC DEFENDER
TENTH JUDICIAL CIRCUIT

TOSHA COHEN
Assistant Public Defender
FLORIDA BAR NUMBER 0022586

Public Defender's Office
Polk County Courthouse
P. O. Box 9000--Drawer PD
Bartow, FL 33831

(863) 534-4200

ATTORNEYS FOR APPELLEE

TOPICAL INDEX TO BRIEF

	<u>PAGE NO.</u>
<u>STATEMENT OF THE CASE AND FACTS</u>	1
<u>SUMMARY OF THE ARGUMENT</u>	5
<u>ARGUMENT</u>	6
<u>ISSUE 6</u>	
IF JURISDICTION EXISTS, THE TRIAL COURT DID NOT ABUSE ITS DISCRETION IN FINDING THAT THE STATE HAD INSUFFICIENT EVIDENCE THAT VIDEO EXISTED, THAT THE PHONE WAS THE CORRECT DEVICE, THAT THE ACT WAS NON-TESTIMONIAL AND THAT THERE WERE NOT LESS INTRUSIVE MEANS TO OBTAIN THIS INFORMATION. (RESTATED BY APPELLEE)	6
<u>CONCLUSION</u>	25
<u>CERTIFICATE OF SERVICE</u>	25

TABLE OF CITATIONS

	<u>PAGE NO.</u>
<u>Federal Cases</u>	
In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F. 3d 1335 (11th Cir. 2011)	passim
S.E.C. v. Huang, Civil Action No. 15-269, 2015 WL 5611644 (E.D. Pennsylvania, September 23, 2015)	21
U.S. v. Fricosu, 841 F. Supp. 2d 1232 (D. Colorado 2012)	20
U.S. v. Kirscher, 823 F. Supp. 2d 665, 668-669 (2010)	21
United State v. Ponds, 454 F3d 313, 320-321 (D.C. Cir 2006)	21
United States v. Doe, 465 U.S. 605, 104 S. Ct. 1237, 79 L.Ed.2d 552 (1984)	20, 21
United States v. Ghidoni, 732 F. 2d 814, 816 (11th Cir. 1984)	19
United States v. Hubbell, 530 U.S. 27, 36, 120 S. Ct. 2037, 2043, 147 L. Ed. 2d 24 (2000)	20
Unlocking a Cellphone, No 14 Mag. 2258, 2014 WL 5510865 (S.D. New York, October 31, 2014)	19
<u>State Cases</u>	
Jones v. State, 477 So. 2d 566, 566 (Fla. 1985)	9
Shaktman v. State, 553 So. 2d 148, 151 (Fla. 1989)	18
State v. G.P., 429 So. 2d 786, 789 (Fla. 3d DCA 1983)	9
State v. Jordan, 783 So. 2d 1179, 1183 (Fla. 3d DCA 2001)	8
State v. MacLeod, 600 So. 2d 1096, 1097 (Fla. 1992)	6
State v. Pettis, 520 So. 2d 250 (Fla. 1988)	9
State v. Smith, 951 So. 2d 954 (Fla. 1st DCA 2007)	12, 13
State v. Storer, 920 So. 2d 754 (Fla. 2d DCA 2006)	12
<u>Rules</u>	
Florida Rule of Appellate Procedure 9.140(c)	6

STATEMENT OF THE CASE AND FACTS

Appellee accepts Appellant's statement of case and facts with the following additions:

The State filed a motion to compel the Defendant to produce his telephone passcode. V1: R22-26. In section (4) of the State's motion to compel, the State asserts the following:

Without compelling the Defendant to provide the passcode, Law Enforcement's only other option is to send the telephone back to the manufacturer to obtain the passcode creating chain of custody issues. V1: R22.

At the motion hearing, the trial court asked:

The Court: How do I know that there was a picture taken?

MS. MEINERS: We don't actually know that a picture has been taken, but we believe that based on the circumstances that there's probable cause to believe one was. V1: T64.

The court then asked about the evidence the State was relying upon for probable cause that a picture was taken. V1: T64. The prosecutor said they were relying on the affidavit. V1: T65. The prosecutor again asserted that they could obtain the same information on the phone through the manufacturer, though it would require special handing to avoid chain of custody issues. V1: T66. The court asked what chain or custody issue was involved, and the prosecutor said that they would have to find out who at the manufacturer handled the phone. V1: T66. The prosecutor had not contacted the manufacturer to find out the process or what

would be involved. V1: R67. The judge then asked the prosecutor if the information could be obtained through law enforcement forensic experts. V1: T66. The prosecutor admitted that they could also possibly obtain the information by running every password combination through the phone. V1: T66. They were not sure if the phone only allowed a limited number of tries because they had not attempted it. V1: T66. The process could take weeks. V1: T67.

The judge did not believe that this issue had not come up in other situations or that the manufacturer would not have an acceptable procedure for this circumstance. V1: T67. With the state of technology and electronic communications, the issues were not too problematic for the State to overcome. V1: T67. The court was not sure the photographs were even on the phone or that they would be accessible if the phone were unlocked. V1: T68. The State conceded that they did not know if any video would be further encrypted in the phone. V1: T68.

The State argued that providing the password code was only testimonial if the State used the fact that Mr. Stahl provided the password and they would not use it because it was not an element of the offense. V1: T71. The court then asked how the State would prove that Mr. Stahl had access to files on the phone. V1: T71. The prosecutor said that they would argue that it was his phone. V1: T71. Mr. Stahl never admitted that he even knew the password on this phone. V1: T72. The prosecutor conceded that in

a technical sense, Mr. Stahl would have to use the contents of his mind to unlock the phone, but argued the caselaw says it does not. V1: T72-73.

The Defense argued that no phone was found on Mr. Stahl's person when he was arrested. V1: T75. The victim stated that she believed the object was a cell phone, not that the object was definitely a cell phone. V1: T75. The search warrant was for a "device" being used. V1: T75. The video did not show a cell phone. V1: T76. There was no evidence that it was the Apple iPhone 5 that they are trying to unlock. V1: T76. It was a leap for officers to hear about a device and then assume it was a specific phone. V1: T76.

The Defense argued that the foregoing conclusion doctrine should not be relied upon because there was not even evidence that officers were trying to break into the right device. V1: T76. There was no evidence that the phone was the correct device or that any video existed on the phone at the time of the motion. V1: T76. The phone was retrieved from a house where multiple people live and there was no evidence that they had the correct phone. V1: T77. There was also no evidence that actual video was taken on any device, including the specific phone. V1: T77. Hoping to find the evidence was not enough. V1: T78. The Defense argued that this was more invasive than unlocking a safe because there are intermingled documents and private information. V1: T78. The new phones are more computer like than old phones. V1:

T78. They can import and export, all sorts of personal information. V1: T78.

The trial court denied the motion to compel. V1: R29. In the order, the court noted that the State represented that they would have to send the phone to the manufacturer if the motion were denied. V1: R30. The trial court was persuaded by the reasoning in In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F. 3d 1335 (11th Cir. 2011), when reaching its decision. V1: T30. The court found that the act of production under these circumstances was testimonial. V1: T30. The court also found that the "reasonable particularity" standard was not met in this case and that there was insufficient evidence that the State already knew all the particulars of the material sought prior to compelling production. V1: R30.

The probable cause affidavit lists the phone as a cell phone, but provides no color, make, model or other identifying feature. V1: R4.

SUMMARY OF THE ARGUMENT

This court should not consider the merits of this appeal because Appellee does not have the right to appeal this issue. The case should be dismissed.

The trial court did not abuse its discretion in denying the motion to compel. The passcode was testimonial. The prosecutor had no specific knowledge of what, if anything, would be found on the phone or if any evidence even exists on any device. The order should be affirmed.

ARGUMENT
ISSUE

IF JURISDICTION EXISTS, THE TRIAL COURT DID NOT ABUSE ITS DISCRETION IN FINDING THAT THE STATE HAD INSUFICIENT EVIDENCE THAT VIDEO EXISTED, THAT THE PHONE WAS THE CORRECT DEVICE, THAT THE ACT WAS NON-TESTIMONIAL AND THAT THERE WERE NOT LESS INTRUSIVE MEANS TO OBTAIN THIS INFORMATION. (RESTATED BY APPELLEE)

There is no jurisdiction to consider the issues in this case. Even if jurisdiction existed, the trial court did not abuse its discretion in this case.

JURISDICTION

The State's right to appeal in a criminal case is available only as provided by statute. See State v. McMahon, 94 So. 3d 468 (Fla. 2012); State v. MacLeod, 600 So. 2d 1096, 1097 (Fla. 1992). Section 924.07(1), Florida Statutes (2011), sets forth the limited circumstances in which the State has a right to appeal. Rule 9.140(c) of the Florida Rules of Appellate Procedure is the procedural counterpart to section 924.07 and lists the types of orders the State may appeal in criminal cases. McMahon, 94 So. 3d at 473. Florida Rule of Appellate Procedure 9.140(c) specifies the limited circumstances wherein the State can appeal an order. The State is appealing under subsection (b) which allows appeals from motions to suppress. The motion being appealed in this case, however, is a motion to compel. The rules limiting the grounds

for State appeals should be strictly construed and other matters cannot be appealed. See Lafave v. State, 149 So. 3d 662 (Fla. 2014) (in the absence of a statutory right to appeal, the State cannot appeal an order).

In the State's Initial Brief, the Attorney General cites to State v. Crumbly, 143 So. 3d 1059 (Fla. 2d DCA 2014) to argue that this Court has jurisdiction. Crumbly, however, is not similar to the instant case. In Crumbly, the trial court sealed medical records obtained through a search warrant. The court ruled that the least intrusive means should be used to access the information. This Court noted that the order sealing the record in that case effectively suppressed the evidence because there was no other way for the State to even view the content of the files.

The situation in the instant case is not the same as in Crumbly. In section (4) of the State's motion to compel, the State asserts the following:

Without compelling the Defendant to provide the passcode, Law Enforcement's only other option is to send the telephone back to the manufacturer to obtain the passcode creating chain of custody issues.

Likewise, the State's position at the August 18, 2014 hearing was that the State could obtain the same information on the phone through the manufacturer, though it would require special handling to avoid chain of custody issues. The judge then asked the prosecutor if the information could be obtained through law enforcement forensic experts. The prosecutor admitted that they

could also possibly obtain the information by running every password combination through the phone. They were not sure if the phone only allowed a limited number of tries because they had not attempted it. The process would only take weeks, which is less time than this appeal will take.

The State had other less intrusive ways to obtain the information from the phone. The State wanted to use the most convenient method and the court rejected this method because it unnecessarily infringed on Mr. Stahl's rights. Other methods were still available that did not impact Appellant's constitutional rights.

This situation is not the same as a court order sealing all the information so that the State could not use it at all. The information, if it exists, is still available through other means. This order is not like an order to suppress because it suppresses nothing. Because it is not the equivalent, the State does not have the right to appeal this motion under section 9.140. As in Lafave, the rules should be strictly construed to limit appeals by the State to those items the legislator specified were appealable matters.

CERTIORARI

The District Courts of Appeal are given certiorari jurisdiction under Article V, section for of the Florida Constitution. Certiorari can be used to gain review of interlocutory orders where the court has departed from the

essential requirements of the law. This applies only to serious error. Also, as the Third District recognized in State v. Jordan, 783 So. 2d 1179, 1183 (Fla. 3d DCA 2001), the State cannot circumvent the absence of a statutory right of appeal through a petition for writ of certiorari. see also State v. Pettis, 520 So. 2d 250 (Fla. 1988). The decision in Jordan also relied on several cases which held that no right of review by certiorari exists if no right of appeal exists. See State v. G.P., 429 So. 2d 786, 789 (Fla. 3d DCA 1983) (where there is no statutory authorization of a state appeal from a final judgment, "certiorari may not be used to circumvent that limitation."); Jones v. State, 477 So. 2d 566, 566 (Fla. 1985) ("The district court erred ... in reviewing by certiorari a case it could not review by appeal.").

In the present case, the order from which the State sought review did not violate a clearly established principle of law. The trial court evaluated the evidence after holding a full hearing before denying the motion. The trial court considered the motion and evidence during this hearing. In section (4) of the State's motion to compel, the State asserts the following:

Without compelling the Defendant to provide the passcode, Law Enforcement's only other option is to send the telephone back to the manufacturer to obtain the passcode creating chain of custody issues.

Likewise, the State's position at the August 18, 2014 hearing was that the State could obtain the same information on the phone through the manufacturer, though it would require special handling

to avoid chain of custody issues. The court asked what chain or custody issue was involved, and the prosecutor said that they would have to find out who at the manufacturer handled the phone. The prosecutor had not contacted the manufacturer to find out the process or what would be involved. The judge then asked the prosecutor if the information could be obtained through law enforcement forensic experts. The prosecutor admitted that they could also possibly obtain the information by running every password combination through the phone. They were not sure if the phone only allowed a limited number of tries because they had not attempted it. The process could take weeks.

The judge did not believe that this issue had not come up in other situations or that the manufacturer would not have an acceptable procedure for this circumstance. With the state of technology and electronic communications, the issues were not too problematic for the State to overcome. This indicates that the trial court believed that there were other less intrusive ways to obtain the same information.

There was also an issue with the sufficiency of the information provided by the State. At the motion hearing, the trial court asked:

The Court: How do I know that there was a picture taken?

MS. MEINERS: We don't actually know that a picture has been taken, but we believe that based on the circumstances that there's probable cause to believe one was. V1: T64.

The court then asked about the evidence the State was relying upon for probable cause that a picture was taken. The prosecutor said they were relying on the affidavit.

The Defense argued that no phone was on Mr. Stahl's person when he was arrested. The victim stated that she believed the object was a cell phone, not that the object was definitely a cell phone. The search warrant was for a "device" being used. The video did not show a cell phone. There was no evidence that it was the Apple iPhone 5 that they are trying to unlock. It was a leap of faith for officers to hear a about device and then assume it was a specific phone.

The trial court was not sure the photographs were even on the phone or that they would be accessible if the phone were unlocked. The State conceded that they did not know if any video would be further encrypted in the phone.

The Defense argued that the foregoing conclusion doctrine should not be relied upon because there was not even evidence that officers were trying to break into the right device. There was no evidence that the location is correct or that video existed on the phone at the time of the motion. The phone was retrieved from a house where multiple people live and there was no evidence that they had the correct phone. There was also no evidence that actual video was taken on any device, including the specific phone. Hoping to find the evidence was not enough. The Defense argued that this was more invasive than unlocking a safe because

there are intermingled documents and private information. The new phones are more computer like than old phones and can import or export all sorts of personal information.

After consideration of all of the issues, the trial court denied the motion to compel. In the order, the court noted that the State represented that they would have to send the phone to the manufacturer if the motion were denied. The trial court found In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F. 3d 1335 (11th Cir. 2011), persuasive when reaching its decision. The court found that the act of production under these circumstances was testimonial. The court also found that the "reasonable particularity" standard was not met in this case and that there was insufficient evidence that the State already knew all the particulars of the material sought prior to compelling production.

The trial court in this case held a full hearing and properly evaluated the evidence both in terms of sufficiency and in terms of the legality of forcing production. The State may not seek certiorari review because it cannot show the circuit court departed from the essential requirements of the law.

Where the trial court does not depart from a clearly established rule of law, there is no certiorari jurisdiction. This Court reached that conclusion in State v. Storer, 920 So. 2d 754 (Fla. 2d DCA 2006). In that case, the trial court excluded reverse Williams Rule type evidence. This Court refused to

"second-guess the trial court" on the issue since the court did not depart from clearly established law.

Likewise, in State v. Smith, 951 So. 2d 954 (Fla. 1st DCA 2007), prior to trial, the trial court excluded collateral crime evidence after evaluating the evidence and finding that the acts were dissimilar. The State filed a writ of certiorari. On appeal, the court noted that writs are meant to be extraordinary and are not the same as interlocutory appeals. These writs are used only to cure the "most serious errors" and not just to correct legal errors. *Id* at 956. Since the court did not apply the wrong procedure, it was not for the appellate court to decide whether the result was correct or incorrect.

This is distinguishable from situations where a writ is filed to protect sensitive information that the trial court has ordered can be discovered. There is no "letting the cat out of the bag" that would be impossible to undo later. It is also different from suppression cases where the trial court completely excludes evidence. The evidence was still available and the trial court just excluded the most invasive way to obtain the information.

In the present case, the trial court did not depart from the essential requirements of the law. Mere disagreement with the result or interpretation of the law is not enough for certiorari jurisdiction. The trial court in this case applied the correct law and reached a legal result. The State had the option of taking the two weeks needed to open the phone another way. The

State may be doing so as this court considers this appeal since the appeal has taken more than two weeks. The fact that the State disagrees with the result does not mean that the trial court departed from the essential requirements of the law or that there was a miscarriage of justice. Because this order did not depart from the essential requirements of the law, the Second District should not take jurisdiction to treat this appeal as a petition for writ of certiorari.

THE TRIAL COURT DID NOT ABUSE ITS DISCRETION

Probable Cause

If this Court does take jurisdiction, then the case should be affirmed because the trial court did not abuse its discretion in this order. Many of these issues have already been touched upon above, but deserve further review if the court chooses to consider the merits of the appeal.

As technology advances, so must laws that protect privacy interests and other civil rights advance to continue to safeguard the citizens of this country. Cell phones have evolved from being just a cordless phone to devices that store personal information, private communications and sensitive credit information. This case arose because there was a code protecting the private information on the phone in question.

The trial court made a thorough inquiry into several matters in this case. The first issue the trial court looked at was whether there was probable cause to believe that there was

evidence on this particular phone. At the motion hearing, the trial court asked:

The Court: How do I know that there was a picture taken?

MS. MEINERS: We don't actually know that a picture has been taken, but we believe that based on the circumstances that there's probable cause to believe one was. V1: T64.

The court then asked about the evidence the State was relying upon for probable cause that a picture was taken. The prosecutor said they were relying on the affidavit. The original description was of a device and did not specify a phone. The probable cause affidavit lists the device as a cell phone, but provides no color, make model or other identifying feature.

The Defense argued that no phone was on Mr. Stahl's person when he was arrested. The victim stated that she believed the object was a cell phone, not that the object was definitely a cell phone. The search warrant was for a "device" being used. The video did not show a cell phone. There was no evidence that it was the specific Apple iPhone 5 that they are trying to unlock. It was a leap for officers to hear a device and then assume it was a specific phone.

The Defense argued that the foregoing conclusion doctrine should not be relied upon because there was not even evidence that officers were trying to break into the right device. There was no evidence that the location is correct or that video existed on the phone at the time of the motion. The phone was retrieved from a

house where multiple people live and there was no evidence that they had the correct phone. There was also no evidence that actual video was taken on any device, including the specific phone. Hoping to find the evidence was not enough. The Defense argued that this was more invasive than unlocking a safe because there are intermingled documents and private information. The new phones are more computer-like than old phones and import or export all sorts of personal information.

The court was not sure any evidence was even on the phone or that it would be accessible if the phone were unlocked. The State conceded that they did not know if any video would be further encrypted in the phone.

The court also found that the "reasonable particularity" standard was not met in this case and that there was insufficient evidence that the State already knew all the particulars of the material sought prior to compelling production. V1: R30.

The State failed to establish that the device described in the affidavit was the phone that they sought to break into. There was no evidence establishing probable cause as to this phone. The trial court was obviously concerned about this issue and looked in detail at the facts supporting the State's request to compel production of the password. The trial court also found that the "reasonable particularity" standard was not met in this case and that there was insufficient evidence that the State already knew all the particulars of the material sought prior to compelling

production.

Assuming there was jurisdiction and assuming that the prosecutor did have sufficient evidence that they had the correct device, the trial court did not abuse its discretion in denying the motion to compel for several reasons:

Privacy Rights

First, as argued above, there were other less intrusive ways for the State to get access to the phone that would not involve forcing Mr. Stahl to provide possibly incriminating information. In section (4) of the State's motion to compel, the State asserts the following:

Without compelling the Defendant to provide the passcode, Law Enforcement's only other option is to send the telephone back to the manufacturer to obtain the passcode creating chain of custody issues.

Likewise, the State's position at the August 18, 2014 hearing was that the State could obtain the same information on the phone through the manufacturer, though it would require special handling to avoid chain of custody issues. The judge then asked the prosecutor if the information could be obtained through law enforcement forensic experts. The prosecutor admitted that they could also possibly obtain the information by running every password combination through the phone. They were not sure if the phone only allowed a limited number of tries because they had not attempted it. The process would only take weeks.

The State had other less intrusive ways to obtain the information from the phone. The State wanted to use the most convenient method and the court said no. Other methods were still available that did not impact Appellant's constitutional rights.

The right to privacy is a fundamental right and is guaranteed by Article I, Section 23 of the Florida Constitution:

Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein. This section shall not be construed to limit the public's right of access to public records and meetings as provided by law.

Unlike Federal law, Florida is very specific about the expectation of privacy. But the right does have some limits. As the court in Shaktman v. State, 553 So. 2d 148, 151 (Fla. 1989), noted:

Like all of our other fundamental rights, the fundamental right of privacy is not absolute. In *Winfield*, the Court found that while a citizen may enjoy a privacy interest in his or her bank records, that privacy interest must yield to the interest of the state under certain circumstances. Justice Adkins, writing for the Court, explained that [t]he right of privacy is a fundamental right which we believe demands the compelling state interest standard. This test shifts the burden of proof to the state to justify an intrusion on privacy. The burden can be met by demonstrating that the challenged regulation serves a compelling state interest and accomplishes its goal through the use of the least intrusive

means. *Winfield*, 477 So.2d at 547 (citations omitted).

The state should be precluded from violating this fundamental right unless there is for a compelling interest and it is as unintrusive as possible. For example, in the case relied upon by the State, State v. Crumbly, 143 So. 3d 1059 (Fla. 2d DCA 2014), the court ruled that the least intrusive means should be used to access the information because of privacy interests.

In the instant case, the trial court properly investigated all possible means of obtaining the information in this case before invading Mr. Stahl's privacy rights. After looking at the evidence, the trial court denied the motion to compel. In the order, the trial court noted that the State had the option of sending the phone to the manufacturer, and feared possible chain of custody issues.

This is not the first phone to ever have possible evidence on it. How do the officers collect evidence when a suspect refuses to unlock a phone? It is possible that industrious officers could run the codes until the code is broken, even though that would take some time. The State conceded it was possible in this case. In a slip copy decision out of New York, In Re Order Requiring [XXX], INC. to Assist in the Execution of a Search Warrant Issued by this Court by Unlocking a Cellphone, No 14 Mag. 2258, 2014 WL 5510865 (S.D. New York, October 31, 2014), a phone company was forced to unlock a phone. This was the less intrusive way to access this information.

In this case, the State had other options in terms of getting access to information on this phone. These other options were less invasive. This supports the trial court's decision in this case because the court was following established law.

Self-incrimination

The trial court also ruled that providing a code for the phone would be testimonial within the meaning of the Fifth Amendment. The Fifth Amendment to the Constitution provides that "[no] person ...shall be compelled in any criminal case to be a witness against himself." This right is also found in Article I, Section 9 of the Florida Constitution.

The protection of the amendment requires that there be compulsion, that the communication or act be testimonial and that it be possibly incriminating. United States v. Ghidoni, 732 F. 2d 814, 816 (11th Cir. 1984). This privilege protects people from their own incriminating testimonial communications. U.S. v. Fricosu, 841 F. Supp. 2d 1232 (D. Colorado 2012). The Fifth Amendment is implicated when production of information compels person to perform an act that may have testimonial aspects and incriminating effects. See United States v. Doe, 465 U.S. 605, 104 S. Ct. 1237, 79 L.Ed.2d 552 (1984). Even where the contents are not privileged, the production act may be. *Id.* For example, there is a testimonial aspect to knowing that the information exists, that the person possesses or controls the information and

that the information is authentic. U.S. v. Fricosu, 841 F. Supp. 2d at 1236 (citing United States v. Hubbell, 530 U.S. 27, 36, 120 S. Ct. 2037, 2043, 147 L. Ed. 2d 24 (2000)). It should be noted that the outcome in Fricosu was different because it involved a defendant who waived her Fifth Amendment rights by acknowledging in an independent conversation that she owned the computer and contents. The officers also had already viewed the files on the computer and were absolutely certain of what they would find in the files because they had already viewed them in legally during a customs inspection. Thus, there would have been independent proof even without the files and there was sufficient evidence that the search was justified.

There are two situations where an act of production may not be testimonial. The first is a situation where the defendant is not called upon to use the contents of his or her mind. An example of this is handing over the key to a safe. The key is not an idea or thought. There is a distinction when information is sought rather than a document, item or sample. See U.S. v. Kirscher, 823 F. Supp. 2d 665, 668-669 (2010) (compelling defendant to provide a password rather than an item, even with limited immunity, still violated his Fifth Amendment rights); S.E.C. v. Huang, Civil Action No. 15-269, 2015 WL 5611644 (E.D. Pennsylvania, September 23, 2015) (password code could not be compelled because it is a thought process and the State did not already know the contents of the testimonial elements). This

exception does not apply to the instant case where Mr. Stahl is being ordered to provide information from his mind rather than an item.

The next exception is the "foregone conclusion" doctrine where the State can show with reasonable particularity evidence that it already knows about the exact materials and any testimonial aspect is a foregone conclusion. See United States v. Doe, 465 U.S. 605, 104 S. Ct. 1237, 79 L. Ed. 2d 552 (1984). This idea hinges on the State having prior knowledge of the existence and location of the information sought. United State v. Ponds, 454 F3d 313, 320-321 (D.C. Cir 2006). In this case, there was no evidence that any video exists. There was no evidence that any incriminating evidence exists on the particular phone in question. The State is doing a fishing expedition hoping that they will find some evidence of some crime and hoping that they have the right device. Because these elements are unknown, the exception for evidence with reasonable particularity does not apply and there is not a foregone conclusion that unlocking the phone will produce any evidence.

In this case, the trial court found In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F. 3d 1335 (11th Cir. 2012), to be persuasive. In that case, a subpoena duces tecum was issued which ordered "John Doe" to produce unencrypted contents to computers and hard drives. The investigation was from evidence that someone had used a YouTube account to share sexual images of

underage girls. The internet protocol (IP) was traced to hotels where Doe had been the sole common registrant. A warrant was issued to search all of his digital media. Some of the material was encrypted. Doe was ordered to turn over unlocked copies of his computers and external hard drives. He refused to comply, asserting his Fifth Amendment right against self-incrimination. The State considered the compliance to be necessary for a public interest and they granted Doe immunity for the production act. Doe refused to comply. The judge held him in contempt of court.

The State thought that data existed in encrypted portions of the hard drive. Proof consisted of random codes that could cloak a large amount of data. The reason the officers thought evidence was in these portions was because it was encoded.

On appeal, the court considered whether the act of production was testimonial and therefore covered by the Fifth Amendment. The court compared *Fisher* and *Hubbell* and determined that in *Fisher*, the production was not testimonial because the State already knew each of the facts that were testimonial from other sources. In *Hubbell*, the act was testimonial because the State only suspected the documents likely existed. The key principle was that "an act of production can be testimonial when that act conveys some explicit or implicit statement of fact that certain materials exist, are in the subpoenaed individual's possession or control, or are authentic." *Id* at 1345. If the material conveys one of these messages and if the individual had to use the content of his

mind, then it is testimonial. *Id.* Applying the principles to the case, the court decided that the act was testimonial in that case and that neither of the exceptions applied. The immunity was insufficient to protect Doe. The contempt order was reversed.

This situation is similar to the instant case, but the State's evidence is even weaker. The State thinks that a device might have been used to take images. There is no evidence of any images being made, only suspicions. A device was present. The State cannot describe the device, but believes it is a phone. From there, the State hoped that it has the right device. The phone may or may not be the correct device. The phone may or may not have images on it. The images may or may not be incriminating. The images may or may not be available for viewing if the code is compelled. Like in *Hubbell*, there is no specific knowledge of the testimonial information. Mr. Stahl is being ordered to use the contents of his mind to access the information on the phone. This would prove that he owned the phone, that he had access to the information on the phone, that they are in his possession and that any evidence was actual footage taken without permission. As in *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, the act is testimonial and is protected by the Fifth Amendment.

Production Immunity

In the instant case, the State asserts that it will not use the fact that Mr. Stahl provided the password and provided a limited immunity. In another *Doe* case, however, it was noted

that:

[T]he Government cannot obtain immunity only for the act of production and then seek to introduce the contents of the production, regardless of whether those contents are characterized as non-testimonial evidence, because doing so would allow the use of evidence derived from the original testimonial statement.

Doe v. United State, 670 F.3d 1335, 1352 (11th Cir. 2012). The granting of immunity in this case is insufficient to protect Mr. Stahl's rights

There is no jurisdiction to take this appeal. Even if there was jurisdiction, the trial court's order should be affirmed and Mr. Stahl should not be compelled to bring testimonial evidence against himself.

CONCLUSION

In light of the foregoing reasons, arguments, and authorities, Appellee respectfully asks this Honorable Court to affirm the order entered by the lower court.

CERTIFICATE OF SERVICE

I certify that a copy has been e-mailed to the Office of the Attorney General at CrimappTPA@myfloridalegal.com, on this 19th day of November, 2015.

CERTIFICATION OF FONT SIZE

I hereby certify that this document was generated by computer using Microsoft Word with Courier New 12-point font in compliance with Fla. R. App. P. 9.210 (a)(2).

Respectfully submitted,

/s/ Tosha Cohen

TOSHA COHEN

Assistant Public Defender
Florida Bar Number 0022586
P. O. Box 9000 - Drawer PD
Bartow, FL 33831
appealfilings@pd10.state.fl.us
tcohen@pd10.state.fl.us
knelson@pd10.state.fl.us

HOWARD L. "REX" DIMMIG, II
Public Defender
Tenth Judicial Circuit
(863) 534-4200

Tjc