IN THE UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES

UNITED STATES, Appellee	)	AMICUS CURIAE BRIEF OF THE UNITED STATES ARMY DEFENSE APPELLATE DIVISION
v.	)	
	)	USCA Dkt. No. 17-0504/AF
Senior Airman (E-4) Hank W. Robinson, United States Air Force, Appellant	)	Crim. App. Dkt. No. ACM 38942

JOSHUA B. FIX
Captain, Judge Advocate
Appellate Defense Counsel
Defense Appellate Division
U.S. Army Legal Services Agency
9275 Gunston Road
Fort Belvoir, VA 22060
(703) 693-0658
joshua.b.fix2.mil@mail.mil
USCAAF Bar No. 36775

CHRISTOPHER D. CARRIER
Lieutenant Colonel, Judge Advocate
Chief, Capital and
Complex Litigation Branch
USCAAF Bar No. 32172

MARY J. BRADLEY
Colonel, Judge Advocate
Chief, Defense Appellate Division
USCAAF Bar No. 30649

Index of Brief

I. WHETHER THE MILITARY JUDGE ABUSED HIS DISCRETION BY FAILING TO SUPPRESS ALL THE EVIDENCE OBTAINED FROM APPELLANT'S CELL PHONE.

II. WHETHER THE AIR FORCE COURT ERRED IN HOLDING APPELLANT WAIVED OBJECTIONS REGARDING INVESTIGATORS EXCEEDING THE SCOPE OF APPELLANT'S CONSENT.

Issues 1

Statement of Statutory Jurisdiction 1

Statement of the Case 1

Statement of Facts 1

Statement of Interest 2

Summary of the Argument 2

Argument 3

I. Origins of the foregone conclusion exception 3

II. Application of foregone conclusion in the federal circuits 6

III. Foregone conclusion as applied to production of digital media. 8

IV. Implications of applying the foregone conclusion exception to custodial interrogation. 13

Table of Authorities[1]

The Constitution of the United States

AMEND V ..... *passim*

United States Supreme Court

Doe v. United States, 487 U.S. 201 (1988) 6

Edwards v. Arizona, 451 U.S. 477 (1981) ..... *passim*

Fisher v. United States, 425 U.S. 391 (1976) ..... *passim*

Hoffman v. United States, 341 U.S. 479 (1951) 10

In re Harris, 221 U.S. 274, 279 (1911) 4

Miranda v. Arizona, 384 U.S. 436 (1966) ..... *passim*

Unites States v. Doe, 465 U.S. 605 (1984) 5

United States v. Hubbell, 530 U.S. 27 (2000) ..... *passim*

United States Court of Appeals for the Armed Forces

United States v. Mitchell, 2017 CAAF LEXIS 856 (C.A.A.F. Aug. 30, 2017) 15

Other United States Courts of Appeals

Butcher v. Bailey, 753 F.2d 465 (6th Cir. 1985) 6

Doe v. United States (In re Grand Jury Subpoena), 383 F.3d 905 (9th Cir. 2004) ... 6

In re Grand Jury Empaneled March 19, 1980, 680 F.2d 327 (3d Cir. 1980) 6

In re Grand Jury Subpoena, 973 F.2d 45 (1st Cir. 1992) 6

[1] Unpublished opinions are attached in the Appendix.

In re Grand Jury Subpoena Duces Tecum Dated October 29, 1992, 1 F.3d 87 (2d Cir. 1992) 6, 9

United States v. Bengivenga, 845 F.2d 593 (5th Cir. 1988) 7-8

United States v. Bright, 596 F.3d 683 (9th Cir. 2010) 13

United States v. Clark, 847 F.2d 1467 (10th Cir. 1988) 6

United States v. Doe (In re Grand Jury Subpoena Duces Tecum), 670 F.3d 1335, (11th Cir. 2012) 11

United States v. Gavegnano, 305 Fed. Appx. 954 (4th Cir. 2009) 11-12, 14

United States v. Ghidoni, 732 F.2d 814 (11th Cir. 1984) 6

United States v. Greenleaf, 546 F.2d 123 (5th Cir. 1977) 6

United States v. Hubbell, 167 F.3d 552 (D.C. Cir. 1999) 6

United States v. Ponds, 454 F.3d 313 (D.C. Cir. 2006) 6

United States v. Porter, 711 F.2d 1397 (7th Cir. 1983) 6

United States v. Rue, 819 F.2d 1488 (8th Cir. 1987) 6

United States v. Stone, 976 F.2d 909 (4th Cir. 1992) 6, 12

United States Trial Courts

In re Grand Jury Subpoena (Boucher), 2007 U.S. Dist. LEXIS 87951 (D. Vt. Nov. 29, 2007) 9-11

In re Grand Jury Subpoena (Boucher), 2009 U.S. Dist. LEXIS 13006 (D. Vt., Feb 19, 2009) 10-11

United States v. Pearson, 2006 U.S. Dist. LEXIS 32982 (N.D. N.Y. May 24, 2006) 8

Statutes, Rules, and Other Authorities

10 U.S.C. § 831 ..... *passim*

Mil. R. Evid. 301(a) 14-15

Mil. R. Evid. 304(b) 14-15

Mil. R. Evid. 305(c)(2) 14-15

Moore's Federal Practice - Civil (2017) 8

Table of All Known Cases Analyzing the Foregone Conclusion Exception with Respect to Digital Media, in Chronological Order

United States v. Pearson, 2006 U.S. Dist. LEXIS 32982, *55-64 (N.D. N.Y. May 24, 2006).

In re Grand Jury Subpoena (Boucher), 2007 U.S. Dist. LEXIS 87951, *13-16 (D. Vt. Nov. 29, 2007).

United States v. Gavegnano, 305 Fed. Appx. 954, 956 (4th Cir. Jan. 16, 2009).

In re Grand Jury Subpoena (Boucher), 2009 U.S. Dist. LEXIS 13006, *6-10 (D. Vt. Feb 19, 2009).

United States v. Fricosu, 841 F. Supp. 2d 1232, 1235-37 (D. Col. 2012).

United States v. Doe (In re Grand Jury Subpoena Duces Tecum), 670 F.3d 1335, 1344-49 (11th Cir. 2012).

Commonwealth v. Gelfgatt, 468 Mass. 512, 523-26 (Mass. 2014).

Commonwealth v. Baust, 89 Va. Cir. 267, 269 (Va. Cir. Ct. 2014).

SEC Civil Action v. Huang, 2015 U.S. Dist. LEXIS 127853 (E.D. Pa. Sep. 23, 2015).

State v. Trant, 2015 Me. Super. LEXIS 272, *7-10 (Me. Super. Ct. Oct. 22, 2015).

United States v. Azarian, 2016 U.S. Dist. LEXIS 109305, *11 (D. Minn. May 18, 2016).

State v. Stahl, 206 So. 3d 124, 136 (Fl. Dist. Ct. App. 2016).

United States v. Apple Mac Pro Computer, 851 F.3d 238, 247-49 (3d Cir. 2017).

Commonwealth v. Jones, 2017 Mass. Super. LEXIS 104, *10 (Mass. Super. Ct. July 25, 2017).

United States v. Robinson, 76 M.J. 663, 669-70 (A.F. Ct. Crim. App. 2017).

IN THE UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES

UNITED STATES, Appellant	)	AMICUS CURIAE BRIEF OF THE UNITED STATES ARMY DEFENSE APPELLATE DIVISION
v.	)	
	)	USCA Dkt. No. 17-0504/AF
Senior Airman (E-4) Hank W. Robinson, United States Air Force Appellee	)	Crim. App. Dkt. No. ACM 38942

TO THE JUDGES OF THE UNITED STATES COURT OF APPEALS FOR THE ARMED FORCES:

Issues Presented

I. WHETHER THE MILITARY JUDGE ABUSED HIS DISCRETION BY FAILING TO SUPPRESS ALL THE EVIDENCE OBTAINED FROM APPELLANT'S CELL PHONE.

II. WHETHER THE AIR FORCE COURT ERRED IN HOLDING APPELLANT WAIVED OBJECTIONS REGARDING INVESTIGATORS EXCEEDING THE SCOPE OF APPELLANT'S CONSENT.

Statement of Statutory Jurisdiction

The amicus adopts the appellant's Statement of Statutory Jurisdiction.

Statement of the Case

The amicus adopts the appellant's Statement of the Case.

Statement of Facts

The amicus adopts the appellant's Statement of Facts.

Statement of Interest

The United States Army Defense Appellate Division files this brief pursuant to Rule 26(a)(1) of this Court's Rules of Practice and Procedures. The Army Defense Appellate Division has an interest in this case because it currently represents at least one client whose case involves a similar issue that is pending a decision before the Army Court of Criminal Appeals. Further, the Defense Appellate Division is likely to represent more clients in future whose cases involve similar issues. This brief is relevant to the disposition of the case because it provides additional law and argument in support of the appellant's brief and position on the issues. Specifically, this brief focuses on the "foregone conclusion" exception to the act of production privilege, and why it is inapplicable to the facts of this case.

Summary of Argument

The "foregone conclusion" exception to the act of production privilege was developed specifically for situations where the act of producing a document in response to a subpoena or court order would implicate the Fifth Amendment. In its opinion below, the Air Force Court of Criminal Appeals [Air Force Court] suggests the foregone conclusion exception is applicable to an involuntary testimonial statement taken in violation of *Edwards v. Arizona*, 451 U.S. 477 (1981). This Court should clarify that the foregone conclusion exception to the act of production privilege does not apply beyond the bounds of the act of production

privilege, and does not apply to violations of *Miranda v. Arizona*, 384 U.S. 436 (1966), *Edwards*, or Article 31, Uniform Code of Military Justice [UCMJ], 10 U.S.C. § 831. Instead, once an *Edwards* violation is established, the Military Rules of Evidence control what exceptions to the exclusionary rule apply.

Argument

The "foregone conclusion" exception to the act of production privilege[2] does not apply to the evidence at issue in this case. The exception was developed as a limit on the act of production privilege, and was not intended for application to actual testimonial statements made in response to custodial interrogation or Article 31 questioning. Applying the foregone conclusion exception outside the context of the act of production privilege would create an exception that swallows the protections of the Fifth Amendment, Article 31, and the Military Rules of Evidence.

I. Origins of the foregone conclusion exception.

The foregone conclusion exception was established to resolve the dilemma when an individual's production of certain specified documents, compelled by a court order, might be seen as violating that individual's right against self-

[2] Various authorities refer to this principle as the "act of production privilege," or the "act of production doctrine." This brief will use the term "privilege" for clarity because some authorities also use the term "doctrine" to refer to the foregone conclusion exception.

incrimination. *Fisher v. United States*, 425 U.S. 391, 394-95 (1974). In *Fisher*, the Supreme Court sought to answer the question "what, if any, incriminating testimony within the Fifth Amendment's protection, is compelled by a documentary summons." *Id.* at 409. The Court acknowledged that even if previously prepared documents are not themselves protected by the Fifth Amendment, "The act of producing evidence in response to a subpoena nevertheless has communicative aspects of its own, wholly aside from the contents of the papers produced. Compliance with the subpoena tacitly concedes the existence of the papers demanded and their possession or control by the taxpayer. It also would indicate the taxpayer's belief that the papers are those described in the subpoena." *Id.* at 410.

The Court determined, however, that such production did not violate the right against self-incrimination under the facts of *Fisher* because, "The existence and location of the papers are a foregone conclusion and the taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers. Under these circumstances by enforcement of the summons 'no constitutional rights are touched. The question is not of testimony but of surrender.'" *Id.* at 411 (quoting *In re Harris*, 221 U.S. 274, 279 (1911)). This passage was the only place in *Fisher* where the term "foregone conclusion" was used, but those two seemingly innocuous words took root in the jurisprudence of

lower courts and became known as the "foregone conclusion exception," or the "foregone conclusion doctrine."

The Supreme Court has seldom revisited the foregone conclusion exception. In 1984, the Court referred to the exception in a footnote to an opinion applying the act of production privilege to preclude an individual from being compelled to produce various documents relating to his businesses. *United States v. Doe*, 465 U.S. 605, 614, n. 13 (1984) [hereinafter "*Doe 1984*"].[3] When the Court finally revisited the foregone conclusion exception directly, it found the exception did not apply when the government seeks a general class of documents without specific knowledge of individual documents. *United States v. Hubbell*, 530 U.S. 27, 44-45 (2000).

In *Hubbell*, the Court distinguished *Fisher*, *inter alia*, because: it was "unquestionably necessary for respondent to make extensive use of 'the contents of his own mind' in identifying the hundreds of documents responsive to the requests in the subpoena. The assembly of those documents was like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a

[3] Because the case law in this area is replete with pseudonymous "Doe" cases, this brief will distinguish between such opinions by reference to the year of publication by the Supreme Court, or, in the case of circuit court of appeals opinions, by reference to the circuit that issued the opinion. The number of "Doe" cases is indicative of the fact that most such cases arise out of motions to quash grand jury subpoenas or similar instruments.

strongbox." *Id.* at 43 (citing *Doe v. United States*, 487 U.S. 201, 210, n. 9 (1988) [*Doe 1988*]).

II. Application of foregone conclusion in the federal circuits.

After *Fisher*, each federal circuit applied or acknowledged the foregone conclusion exception in the context of the act of production privilege. *See, e.g.*, *In re Grand Jury Subpoena*, 973 F.2d 45, 51 (1st Cir. 1992); *In re Grand Jury Subpoena Duces Tecum Dated October 29, 1992*, 1 F.3d 87, 93 (2d Cir. 1992)[*Doe 2d Cir.*]; *In re Grand Jury Empaneled March 19, 1980*, 680 F.2d 327, 335 (3d Cir. 1980)(*rev'd in part* by *Doe 1984*); *United States v. Stone*, 976 F.2d 909, 911 (4th Cir. 1992); *United States v. Greenleaf*, 546 F.2d 123, 126, n. 7 (5th Cir. 1977); *Butcher v. Bailey*, 753 F.2d 465, 469 (6th Cir. 1985); *United States v. Porter*, 711 F.2d 1397, 1400-01 (7th Cir. 1983); *United States v. Rue*, 819 F.2d 1488, 1492 (8th Cir. 1987); *Doe v. United States (In re Grand Jury Subpoena)*, 383 F.3d 905, 910 (9th Cir. 2004); *United States v. Clark*, 847 F.2d 1467, 1472-73 (10th Cir. 1988); *United States v. Ghidoni*, 732 F.2d 814, 817 (11th Cir. 1984); *United States v. Ponds*, 454 F.3d 313, 324 (D.C. Cir. 2006).

The decision of the Court of Appeals for the D.C. Circuit in *United States v. Hubbell*, 167 F.3d 552 (D.C. Cir. 1999)(*aff'd Hubbell*, *supra*), is emblematic of the view of the foregone conclusion exception as it developed in the various circuits.

In this view, the exception applies to the act of production privilege, when asserted in response to a subpoena, if the government can meet several burdens:

> [T]he government must establish its knowledge of the existence, possession, and authenticity of subpoenaed documents with reasonable particularity before the communication inherent in the act of production can be considered a foregone conclusion. In making this assessment, though, the focus must remain upon the degree to which a subpoena invades the dignity of the human mind, and on the quantum of information as to the existence, possession, or authenticity of the documents conveyed via the act of production.

Id. at 579-80 (internal citations, quotation marks, and footnotes omitted).

As far as the undersigned counsel have found, all published cases from the United States district courts and the circuit courts of appeals addressing the foregone conclusion exception do so in the context of the act of the production privilege. Further, out of dozens of published federal civilian cases applying the foregone conclusion exception, the undersigned counsel find only one that applied the exception to a custodial interrogation. In *United States v. Bengivenga*, 845 F.2d 593 (5th Cir. 1988), the court found that the act of producing a bus ticket in response to a border patrol agent's question was nontestimonial, and even if it were testimonial, the foregone conclusion exception would apply. *Id.* at 600-01. As the foregone conclusion exception appears to only provide an alternative basis for the court's holding, the precedential value of this assertion is unclear and the analysis

supporting it is scant. This Court should not rely on *Bengivenga* because it is an anomalous island in the sea of foregone conclusion jurisprudence.

Other than in *Bengivenga*, published opinions from the federal civilian courts addressing the foregone conclusion exception appear consistent with the explanation of the exception provided in *Moore's Federal Practice*, which describes it wholly in relation to the act of production privilege.

> When the existence and location of documents are a 'foregone conclusion,' an individual generally cannot rely on the theory that the 'act of production' itself would be incriminating. For the 'foregone conclusion' exception to apply, the party seeking production (usually the government) must establish its independent knowledge of three elements: the documents' existence, the documents' authenticity, and the respondent's possession or control of the documents.

6-26 *Moore's Federal Practice - Civil* § 26.51 (2017).

III. Foregone conclusion as applied to production of digital media.

As the world transitioned from storing information primarily in paper files to storing information primarily in a digital form, courts began to apply the foregone conclusion exception to the act of production privilege as to digital media. The first instance of this appears to be *United States v. Pearson*, 2006 U.S. Dist. LEXIS 32982 (N.D. N.Y. May 24, 2006). In *Pearson*, the court found that the foregone conclusion exception could potentially apply to defeat an accused's act of production privilege as to certain computer files subpoenaed by the government.

Id. at *55-62. The court did not fully decide the issue in its written opinion, however, and instead set a hearing to make factual findings as to whether all testimonial aspects of the production were already known to the government.

The next case to address the foregone conclusion exception in the digital context was *In re Grand Jury Subpoena (Boucher)*, 2007 U.S. Dist. LEXIS 87951 (D. Vt. Nov. 29, 2007)[*Boucher I*]. In *Boucher I*, the court found that the foregone conclusion exception did not apply when the government sought production of the accused's digital password.

> Since the government is trying to compel the production of the password itself, the foregone conclusion doctrine cannot apply. The password is not a physical thing. If Boucher knows the password, it only exists in his mind. This information is unlike a document, to which the foregone conclusion doctrine usually applies, and unlike any physical evidence the government could already know of. It is pure testimonial production rather than physical evidence having testimonial aspects. Compelling Boucher to produce the password compels him to display the contents of his mind to incriminate himself. [*Doe 2d Cir.*] did not deal with production of a suspect's thoughts and memories but only previously created documents. The foregone conclusion doctrine does not apply to the production of non-physical evidence, existing only in a suspect's mind where the act of production can be used against him.

Boucher I at *16.

The government appealed the ruling from *Boucher I*,[4] but modified its requested relief to seek only the production of unencrypted versions of the files in question, rather than the password needed to unencrypt the files. Under this new theory, the court reversed the earlier result and found the foregone conclusion exception applied to the production of the digital files themselves, which the accused had already shown, at least in part, to a law enforcement agent. *In re Grand Jury Subpoena (Boucher)*, 2009 U.S. Dist. LEXIS 13006, * 1-2, 9-10 (D. Vt. Feb. 19, 2009) (*Boucher II*). The opinion in *Boucher II*, however, failed to account for the "link in the chain" principle articulated in *Hoffman v. United States*, 341 U.S. 479, 486 (1951), and later adopted and expanded in *Hubbell*, 341 U.S. at 38 ("testimony that communicates information that may lead to incriminating evidence is privileged even if the information itself is not inculpatory.")(internal quotes omitted).

The *Boucher II* opinion also seems to have discounted the requirement that the government already have actual knowledge that particularized documents exist. Instead, the court found the government met the knowledge prong of the test by showing it knew documents in general existed in the custody of the suspect. *See Boucher II* at *9. This is little different from the situation in *Hubbell*, however,

---

[4] The ruling in *Boucher I* was by a magistrate judge authorized to conduct the hearing. As a result, the appeal was to the District Court itself, which reviewed the issue de novo. *Boucher II*, at * 2-3.

which the Supreme Court found did not fall under the foregone conclusion exception. *See Hubbell*, 341 U.S. at 44-45.

Nevertheless, the juxtaposition between *Boucher I* and *Boucher II*, is useful to show that, since the earliest cases applying the foregone conclusion exception to digital media, courts understood it strictly as an exception to the act of production privilege. Courts have not applied it as an exception to the privilege against making actual testimonial statements, whether written or oral, which are incriminating.

The first time a federal circuit court of appeals weighed in on the issue of the foregone conclusion exception to the act of production privilege for digital media was the landmark case of *United States v. Doe (In re Grand Jury Subpoena Duces Tecum)*, 670 F.3d 1335 (11th Cir. 2012) [*Doe 11 Cir.*]. In *Doe 11th Cir.*, the court conducted a thorough review of the foregone conclusion exception, spanning several written pages, and determined it was not applicable to the compelled production of the unencrypted contents of several digital storage devices. *Id.* at 1344-49.

Contrasting with the outcome and the thorough analysis of *Doe 11th Cir.* is the Fourth Circuit's cursory unpublished opinion in *United States v. Gavegnano*, 305 Fed. Appx. 954 (4th Cir. 2009). In *Gavegnano*, the court stated, without further analysis:

> Gavegnano's Fifth Amendment claim, based on the fact that, after invoking his right to consult with an attorney, he was asked for, and revealed, the password to the computer, also fails. Any self-incriminating testimony that he may have provided by revealing the password was already a 'foregone conclusion' because the Government independently proved that Gavegnano was the sole user and possessor of the computer.

Id. at 956 (citing *United States v. Stone*, 976 F.2d 909, 911 (4th Cir. 1992) (an act of production case) (quoting *Fisher*, 425 U.S. at 411).

The Air Force Court relied upon *Gavegnano*, at least in part, in its opinion below. Because *Gavegnano* is an unpublished opinion, however, the Air Force Court has the distinction of being the first and only court to issue a published opinion suggesting the foregone conclusion exception may be applied to a testimonial statement made in response to custodial interrogation.

Unfortunately, the Air Force Court was wrong to rely on *Gavegnano* because the foregone conclusion exception is an exception to the act of production privilege, not to the privilege against making actual involuntary statements in response to custodial interrogation. Further, the foregone conclusion exception was developed to apply in cases where the act of production privilege is asserted in response to a subpoena or motion to compel production, not to cases involving in-person interrogation, particularly in-person interrogation that persists after a suspect has invoked his or her right to counsel.

A marked difference exists between statements made during custodial interrogation or Article 31 questioning, and documents produced in response to a subpoena or motion to compel production. During custodial interrogation, at least in this case, no counsel was present despite the appellant's request for one. By contrast, when the government seeks a document through a subpoena or motion to compel production, the person from whom the document is sought may, through counsel, move to quash the subpoena or deny the motion as the many *Doe* cases illustrate.

The foregone conclusion exception was never intended to apply outside the act of production privilege or outside the judicially supervised processes of subpoenas and motions to compel production. As the Ninth Circuit has explained, "The application of privilege to a document production is different from a blanket privilege claim at an interview. An unscripted interview is undefined, so a court cannot make a reasoned assessment of privilege before particular questions have been posed." *United States v. Bright*, 596 F.3d 683, 691 (9th Cir. 2010).

IV. Implications of applying the foregone conclusion exception to custodial interrogation.

The path of applying the foregone conclusion exception beyond the act of production privilege and outside the judicially supervised processes of subpoenas and motions to compel production, if followed, would lead to the abrogation of the Fifth Amendment and Article 31. Once set free from the intended confines of the

act of production privilege, the foregone conclusion exception would operate like an invasive species overtaking the protections of *Miranda*, *Edwards*, and Article 31.

A hypothetical is useful to illustrate why the foregone conclusion exception is inappropriate to custodial interrogations and inappropriate outside the act of production privilege: Suppose farmer Jones is suspected of shooting his neighbor with his pistol. Suppose further that Jones is well-known to own a pistol, and this fact is not in dispute, but the police cannot locate the firearm on Jones' vast farm. The police take Jones into custody and ask him about the shooting. In response, Jones states he wants to see his lawyer. The police do not honor this request, however, and instead ask Jones where he has hidden his pistol. Jones relents and admits that the pistol is buried under the old oak tree on his back forty acres.

Under the Air Force Court's adoption of *Gavegnano*, the foregone conclusion exception would prevent farmer Jones from suppressing his involuntary statement to the police and the firearm derived therefrom. This result is contrary to *Edwards* and, in the military system, contrary to Mil. R. Evid. 305(c)(2).

As a judicially-created exception, applicable in narrow situations in the civilian justice system, the foregone conclusion exception is not compatible with Mil. R. Evid. 301(a), 304(b), or 305(c)(2). Military Rule of Evidence 305(c)(2) requires suppression of evidence acquired in violation of *Edwards*, subject only to

the exceptions explicitly provided in Mil. R. Evid. 304(b). Even if the foregone conclusion exception otherwise applied as an exception to the exclusionary rule in general, and not just to the act of production privilege, the Military Rules of Evidence provide, "An individual may claim the most favorable privilege provided by the Fifth Amendment to the United States Constitution, Article 31, *or these rules*." Mil. R. Evid. 301(a)(emphasis added). "Under the plain language of the Military Rules of Evidence, any evidence derived from a violation of *Edwards* must be suppressed." *United States v. Mitchell*, 2017 CAAF LEXIS 856, *14 (C.A.A.F. Aug. 30, 2017). Thus, applying the foregone conclusion exception to violations of *Miranda*, *Edwards*, and Article 31,[5] is incompatible with the Military Rules of Evidence, and the Air Force Court's suggestion to the contrary is in error.

The origins and development of the foregone conclusion exception demonstrate that it is a narrow exception, only applicable to the act of production privilege, and only appropriate in the context of judicially supervised exchanges, such as subpoenas and motions to compel production. Further, the foregone conclusion exception would be incompatible with the Military Rules of Evidence if applied to involuntary statements.

---

[5] With respect to *Miranda* and Article 31 violations, Mil. R. Evid. 304(a) applies to require suppression of the evidence, but the principle is the same as articulated for Mil. R. Evid. 305(c)(2) in *Mitchell*.

For these reasons, this Court should explicitly hold the foregone conclusion exception does not apply to evidence obtained in violation of Article 31, *Miranda*, or *Edwards*.

Conclusion

WHEREFORE, the amicus respectfully requests that this Honorable Court set aside the ruling below.

JOSHUA B. FIX
Captain, Judge Advocate
Appellate Defense Counsel
Defense Appellate Division
U.S. Army Legal Services Agency
9275 Gunston Road
Fort Belvoir, VA 22060
(703) 693-0658
joshua.b.fix2.mil@mail.mil
USCAAF Bar No. 36775

CHRISTOPHER D. CARRIER
Lieutenant Colonel, Judge Advocate
Chief, Capital and
Complex Litigation Branch
USCAAF Bar No. 32172

MARY J. BRADLEY
Colonel, Judge Advocate
Chief, Defense Appellate Division
USCAAF Bar No. 30649

Certificate of Compliance with Type-Volume Limitations

1. This brief complies with the type-volume limitations of Rules 24(c) and 26(f) because it contains 3,400 words.

2. This brief complies with the typeface and type style requirements of Rule 37 because it has been prepared in Times New Roman font, using 14-point type with one-inch margins.

JOSHUA B. FIX
Captain, Judge Advocate
Appellate Defense Counsel
9275 Gunston Road
Fort Belvoir, Virginia 22060-5546
(703) 693-0658
USCAAF No. 36775

CERTIFICATE OF FILING AND SERVICE

I certify that a copy of the foregoing in the case of *United States v. Robinson,* Dkt. No. ACM 38942, USCA Dkt. No. 17-0504/AF, was electronically filed brief with the Court and Government Appellate Division on September 25, 2017.

MICHELLE L. WASHINGTON
Paralegal Specialist
Defense Appellate Division
(703) 693-0737

APPENDIX

LexisNexis®

UNITED STATES OF AMERICA, Plaintiff - Appellee, v. DEREK F. GAVEGNANO, Defendant - Appellant.

No. 07-4579

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

305 Fed. Appx. 954*; *2009 U.S. App. LEXIS 844

October 28, 2008, Submitted
January 16, 2009, Decided

NOTICE: PLEASE REFER TO FEDERAL RULES OF APPELLATE PROCEDURE RULE 32.1 GOVERNING THE CITATION TO UNPUBLISHED OPINIONS.

SUBSEQUENT HISTORY: Summary judgment denied by, Post-conviction relief dismissed at, Certificate of appealability denied *United States v. Gavegnano, 2012 U.S. Dist. LEXIS 70933 (W.D. Va., May 21, 2012)*

PRIOR HISTORY: [**1]

Appeal from the United States District Court for the Western District of Virginia, at Charlottesville. (3:05-cr-00017-nkm). Norman K. Moon, District Judge.

United States v. Gavegnano, 2007 U.S. Dist. LEXIS 18269 (W.D. Va., Mar. 15, 2007)

DISPOSITION: AFFIRMED.

COUNSEL: Michael T. Hemenway, THE LAW OFFICES OF MICHAEL T. HEMENWAY, Charlottesville, Virginia, for Appellant.

Julia C. Dudley, Acting United States Attorney, Jean B. Hudson, Assistant United States Attorney, Charlottesville, Virginia, for Appellee.

JUDGES: Before MOTZ, TRAXLER, and SHEDD, Circuit Judges.

OPINION

[*955] PER CURIAM:

Derek F. Gavegnano appeals his conviction on two counts of receipt of child pornography, in violation of *18 U.S.C. §§ 2252(a)(2), 3261(a) (2006)*; one count of possession of child pornography, in violation of *18 U.S.C. §§ 2252(a)(4), 3261(a) (2006)*; and one count of importation or transportation of obscene matters, in violation of *18 U.S.C. §§ 1462, 3261(a) (2006)*. We have reviewed the record and find no reversible error.

Gavegnano first claims the district court erred in denying his motion to suppress based on violation of his *Fourth* and *Fifth Amendment* rights when evidence against him was obtained from a government-issued laptop. We review legal conclusions underlying the denial of a motion to suppress de novo, and review factual

[**2] findings for clear error. *United States v. Moreland, 437 F.3d 424, 433 (4th Cir. 2006)*. The evidence is construed in the light most favorable to the Government. *United States v. Seidman, 156 F.3d 542, 547 (4th Cir. 1998)*.

To establish a violation of his *Fourth Amendment* rights, Gavegnano must establish that he had a "legitimate expectation of privacy" in the computer searched. *United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000)* (citing *Rakas v. Illinois, 439 U.S. 128, 143, 99 S. Ct. 421, 58 L. Ed. 2d 387 (1978))*. To prove a legitimate expectation of privacy, Gavegnano must show that his subjective expectation of privacy is one that society is prepared to accept as objectively reasonable. *Simons, 206 F.3d at 398*. As the district court properly held, this he did not do.

It is uncontroverted that when Gavegnano was issued a government computer, the user agreement he signed stated that he was aware of the acceptable use of all government-issued information systems, [*956] that he consented to the monitoring of the information systems, and included the statement that he understood that monitoring was not selective and would include all activities on the information system. Moreover, the user agreement form Gavegnano signed [**3] applied to his use of all computer systems owned by the governmental agency for which he worked, which included the laptop he used in Qatar, on which the pornographic images were found. On these facts, and construing the evidence in favor of the Government, see *Seidman, 156 F.3d at 547*, we find no clear error by the district court in its determination that Gavegnano had no reasonable expectation of privacy in the unauthorized use of his government-issued laptop computer such that his *Fourth Amendment* rights were violated.

Gavegnano's *Fifth Amendment* claim, based on the fact that, after invoking his right to consult with an attorney, he was asked for, and revealed, the password to the computer, also fails. Any self-incriminating testimony that he may have provided by revealing the password was already a "foregone conclusion" because the Government independently proved that Gavegnano was the sole user and possessor of the computer. See *United States v. Stone, 976 F.2d 909, 911 (4th Cir. 1992)* (quoting *Fisher v. United States, 425 U.S. 391, 411, 96 S. Ct. 1569, 48 L. Ed. 2d 39 (1976))*.

Next, Gavegnano challenges the district court's taking of judicial notice of the court's jurisdiction insofar as its failure to instruct [**4] the jury that it was not required to accept as conclusive any fact judicially noticed, as required by *Fed. R. Evid. 201(g)*. Specifically, he takes issue with the district court's judicial notice that Gavegnano was charged with crimes punishable by over a year in prison.

Rule 201(a) limits the scope of *Rule 201* to judicial notice of adjudicative, not legislative, facts. See *Fed. R. Evid. 201(a)* advisory committee notes. Here, the fact of which the district court took judicial notice, i.e., the penalty for the crimes with which Gavegnano was charged, is fixed, does not change from case to case, and applies to all cases in which those crimes were charged. Hence, it is a legislative, not an adjudicative fact. See, e.g., *United States v. Williams, 442 F.3d 1259, 1261 (10th Cir. 2006)* (citations omitted) ("statutes are considered legislative facts" of which the authority of courts to take judicial notice is "unquestionable."). Accordingly, the district court was under no obligation to follow the jury instruction requirement set out in *Rule 201(g)*, and it committed no reversible error in its failure to instruct the jury pursuant to *Rule 201(g)*.

In a related claim, Gavegnano also challenges [**5] the district court's taking of judicial notice of the element that the crimes with which he was charged were punishable by more than one year in prison if committed in the United States, an element required under *18 U.S.C. § 3261*, claiming that the court's action precluded him from requiring that the Govern-

ment prove each element of the charges against him beyond a reasonable doubt. He supports his argument by reference to Virginia state law statutes regarding obscene material that carry sentences of less than a year. He also asserts that one of the charges carried a penalty of "zero to five" years. His argument is without merit.

First, as discussed above, the district court properly may take judicial notice of legislative facts, and such legislative facts include the interpretation of statutes. *Fed. R. Evid. 201(a)* advisory comm. notes. Moreover, the requirements of *Rule 201(b)* state that a "judicially noticed fact must be one that is either (1) generally known within the territorial jurisdiction of the trial court, or (2) capable of accurate and [*957] ready determination by resort to sources whose accuracy cannot reasonably be questioned." Here, the length of punishment is determined simply [**6] by reading the text of the statutes violated, each of which provide that violation of the statute is punishable by more than one year in prison. *

> * Counts One through Six of which Gavegnano was charged alleged a violation of *18 U.S.C. § 2252(a)(2)*, requiring a punishment of five to twenty years in prison. See *18 U.S.C. § 2252(b)(1) (2006)*. Count Seven, alleging a violation of *18 U.S.C. § 2252(a)(4)*, is punishable by up to ten years in prison. See *§ 2252(b)(2)* (2006). Count Eight, alleging a violation of *18 U.S.C. § 1462 (2006)*, is punishable by up to five years in prison.

Second, Gavegnano's reliance on the fact that certain Virginia state statutes provide for punishment of less than a year for the receipt and possession of obscene material is misplaced, as Gavegnano was not charged under Virginia law, but rather under federal statutes for offenses that took place in Qatar. As it is undisputed that, on their face, the federal statutes under which Gavegnano was charged carried sentences of more than one year, the length of the relevant penalties cannot reasonably be questioned. Hence, the fact of that penalty properly was found by judicial notice.

Likewise without merit is Gavegnano's [**7] contention that judicial notice was not proper because one of the charges carried a penalty of "zero to five" years. As the crimes all were *punishable* by imprisonment for a term exceeding one year, the actual prison sentence imposed is not relevant to the determination of whether judicial notice in this case was proper. See e.g., *United States v. Jones, 195 F.3d 205, 207 (4th Cir. 1999)*.

Gavegnano's additional assertion, that by taking judicial notice the district court erroneously precluded him from requiring the Government to meet its burden of proof for the element of *§ 3261* requiring the alleged crimes to carry a prison sentence of over a year, is without merit. As the length of the penalty properly was a judicially noticed fact, the Government was without obligation to prove that element, and we find no error.

Gavegnano's final claim on appeal is that the district court erred in admitting the forensic report which detailed the contents of the computer containing child pornography. His objection is based on his contention that the chain of custody for the computer had not been adequately established because other individuals handled the computer after it was taken away from him, [**8] such that tampering could have occurred.

Pursuant to *Fed. R. Evid. 901(a)*, a party introducing evidence is required to authenticate it with "evidence sufficient to support a finding that the matter in question is what its proponent claims." The proper inquiry relating to chain of custody is whether the authentication testimony was sufficient to "convince the court that it is improbable that the original item had been exchanged with another or otherwise tampered with." *United States v. Howard-Arias, 679 F.2d*

363, 366 (4th Cir. 1982) (citation omitted). Chain of custody precision is not an "iron-clad requirement" and a "missing link does not prevent the admission of real evidence, so long as there is sufficient proof that the evidence is what it purports to be and has not been altered in any material aspect." Id. (internal quotation marks and citation omitted). Once evidence is established that the item is what it is purported to be any "[r]esolution of whether evidence is authentic calls for a factual determination by the jury. . . ." *United States v. Branch, 970 F.2d 1368, 1370 (4th Cir. 1992)*. It is the jury's job to evaluate any defects in the chain of custody and accept or disregard [**9] evidence. *United States v. Clonts, 966 F.2d 1366, 1368* [*958] *(10th Cir. 1992)*. The decision to admit evidence at trial is within the sound discretion of the district court and we review for abuse of discretion. *United States v. Jones, 356 F.3d 529, 535 (4th Cir. 2004)*.

Here, the Government satisfied its *Rule 901(a)* burden. Evidence was introduced that the forensic report contained information found on Gavegnano's computer. Evidence was presented that matched the serial number for the computer subject to the forensic report with the computer and hard drive issued to Gavegnano. Gavegnano admitted that the computer placed into evidence, which was the same computer from which the files listed in the forensic report were taken, was the same one taken from him in Qatar. The Government introduced testimony by the man who saw pornography on Gavegnano's computer before it was taken by the Government. There was no evidence or indication of any tampering with the computer between the time it was taken from Gavegnano and the time the forensic report was compiled. That others looked at or used Gavegnano's computer during the time it was in custody, and the possibility that they may have tampered with [**10] the computer, was an issue for the jury to consider. See *Branch, 970 F.2d at 1370*. We find no abuse of the district court's discretion when it found the Government had established a sufficient chain of custody and admitted the forensic report.

Accordingly, we affirm Gavegnano's conviction and sentence. We dispense with oral argument because the facts and legal contentions are adequately presented in the materials before the court and argument would not aid the decisional process.

AFFIRMED

In re: Grand Jury Subpoena to Sebastien Boucher

No. 2:06-mj-91

UNITED STATES DISTRICT COURT FOR THE DISTRICT OF VERMONT

2007 U.S. Dist. LEXIS 87951

November 29, 2007, Decided
November 29, 2007, Filed

SUBSEQUENT HISTORY: Reversed by, Motion denied by, Objection sustained by *In re Grand Jury Subpoena (Boucher), 2009 U.S. Dist. LEXIS 13006 (D. Vt., Feb. 19, 2009)*

DISPOSITION: Motion to quash recommended to be granted.

COUNSEL: [*1] For Sebastien D. Boucher, Defendant (1): Bradley S. Stetler, LEAD ATTORNEY, Stetler, Allen & Kampmann, Burlington, VT; James H. Budreau, LEAD ATTORNEY, Law Office of James Budreau, Boston, MA.

For USA, Plaintiff: Paul J. Van de Graaf, LEAD ATTORNEY, Office of the United States Attorney District of Vermont, Burlington, VT.

JUDGES: Jerome J. Niedermeier, United States Magistrate Judge.

OPINION BY: Jerome J. Niedermeier

OPINION

OPINION AND ORDER

(Paper 14)

On December 17, 2006, defendant Sebastien Boucher was arrested on a complaint charging him with transportation of child pornography in violation of *18 U.S.C. § 2252A(a)(1)*. At the time of his arrest government agents seized from him a laptop computer containing child pornography. The government has now determined that the relevant files are encrypted, password-protected, and inaccessible. The grand jury has subpoenaed Boucher to enter a password to allow access to the files on the computer. Boucher has moved to quash the subpoena on the grounds that it violates his *Fifth Amendment* right against self-incrimination. On July 9, 2007 and November 1, 2007, the Court held evidentiary hearings on the motion.

Background

On December 17, 2006, Boucher and his father crossed the [*2] Canadian border into the United States at Derby Line, Vermont. At the border station, agents directed Boucher's car into secondary inspection. Customs and

Border Protection Officer Chris Pike performed the secondary inspection.

Officer Pike found a laptop computer in the back seat of the car. He opened the computer and accessed the files without entering a password. Officer Pike conducted a search of the computer files for any images or videos. He located approximately 40,000 images, some of which appeared to be pornographic based on the names of the files.

Officer Pike asked Boucher whether any of the image files on the laptop contained child pornography. Boucher responded that he was uncertain, and Officer Pike continued investigating the contents of the computer. Officer Pike noticed several file names that appeared to reference child pornography. He then called Special Agent Mark Curtis of Immigration and Customs Enforcement who has experience and training in recognizing child pornography.

When Agent Curtis arrived, he examined the computer and found a file named "2yo getting raped during diaper change." Agent Curtis was unable to open the file to view it. However, Agent Curtis determined [*3] that the file had been opened on December 11, 2006. He continued to investigate and found thousands of images of adult pornography and animation depicting adult and child pornography.

Agent Curtis then read Boucher his Miranda rights. Boucher waived his rights in writing and agreed to speak to Agent Curtis. Agent Curtis asked Boucher about the file "2yo getting raped during diaper change." Boucher stated that he downloads many pornographic files from online newsgroups onto a desktop computer at home and then transfers them to his laptop. Boucher also stated that he sometimes unknowingly downloads images that contain child pornography but deletes them when he realizes their contents.

Agent Curtis asked Boucher to show him where the files he downloaded from the newsgroups were located on the laptop. Boucher was allowed access to the laptop and navigated to a part of the hard drive designated as drive Z. Agent Curtis did not see Boucher enter a password to access drive Z. Agent Curtis began searching through drive Z in Boucher's presence though Boucher appeared to be uncomfortable with this.

Agent Curtis located many adult pornographic files and one video entitled "preteen bondage." Agent [*4] Curtis viewed the video and observed what appeared to be a preteen girl masturbating. He asked Boucher whether he had any similar files on his laptop, and Boucher again stated that he usually deletes files that he discovers to contain child pornography.

Agent Curtis then asked Boucher to leave the room and continued to examine drive Z. He located several images and videos of child pornography in drive Z. After consulting with the United States Attorney's office, Agent Curtis arrested Boucher. He then seized the laptop, after shutting it down.

On December 29, 2006, Mike Touchette of the Vermont Department of Corrections took custody of the laptop. Touchette created a mirror image of the contents of the laptop. When Touchette began exploring the computer, he could not access drive Z because it was protected by encryption algorithms through the use of the software Pretty Good Privacy ("PGP"), which requires a password to access drive Z. Since shutting down the laptop, the government has been unable to access drive Z to view the images and videos containing child pornography.

Secret Service Agent Matthew Fasvlo, who has experience and training in computer forensics, testified that it is nearly [*5] impossible to access these encrypted files without knowing the password. There are no "back doors" or secret entrances to access the files. The only way to get access without the password is to use an automated system which repeatedly guesses passwords. According to the government, the

process to unlock drive Z could take years, based on efforts to unlock similarly encrypted files in another case. Despite its best efforts, to date the government has been unable to learn the password to access drive Z.

To gain access to drive Z and the files in question, the grand jury has subpoenaed Boucher directing him to:

> provide all documents, whether in electronic or paper form, reflecting any passwords used or associated with the Alienware Notebook Computer, Model D9T, Serial No. NKD900TA5L00859, seized from Sebastien Boucher at the Port of Entry at Derby Line, Vermont on December 17, 2006.

Boucher has moved to quash the subpoena as violative of his *Fifth Amendment* right against self-incrimination. At the hearing the government suggested that Boucher could enter the password into the computer without the government, the grand jury, or the Court observing or recording the password in any way. The [*6] government also suggested that to avoid any *Fifth Amendment* issue the Court could order that the act of entering the password could not be used against Boucher. The Court must now determine whether compelling Boucher to enter the password into the laptop would violate his *Fifth Amendment* privilege against self-incrimination.

Discussion

The *Fifth Amendment* privilege against self-incrimination "protects a person ... against being incriminated by his own compelled testimonial communications." *Fisher v. United States, 425 U.S. 391, 409, 96 S. Ct. 1569, 48 L. Ed. 2d 39 (1976)*. For the privilege to apply, the communication must be compelled, testimonial, and incriminating in nature. *Id. at 408*. Subpoenas require compliance and therefore constitute compulsion. *Id. at 409* (stating that a subpoena requiring production of evidence "without doubt involves substantial compulsion."). Because the files sought by the government allegedly contain child pornography, the entry of the password would be incriminating. Whether the privilege against self incrimination applies therefore depends on whether the subpoena seeks testimonial communication.

Both parties agree that the *contents* of the laptop do not enjoy *Fifth Amendment* protection as [*7] the contents were voluntarily prepared and are not testimonial. *See id. at 409-10* (holding previously created work documents not privileged under the *Fifth Amendment*). Also, the government concedes that it cannot compel Boucher to disclose the password to the grand jury because the disclosure would be testimonial. The question remains whether entry of the password, giving the government access to drive Z, would be testimonial and therefore privileged.

I. Entering the Password is Testimonial

Compelling Boucher to enter the password forces him to produce evidence that could be used to incriminate him. Producing the password, as if it were a key to a locked container, forces Boucher to produce the contents of his laptop.

The act of producing even unprivileged evidence can have communicative aspects itself and may be "testimonial" and entitled to *Fifth Amendment* protection. *United States v. Doe, 465 U.S. 605, 612, 104 S. Ct. 1237, 79 L. Ed. 2d 552 (1984)* [hereinafter *Doe I*] ("Although the contents of a document may not be privileged, the act of producing the document may be."). An act is testimonial when the act entails implicit statements of fact, such as admitting that evidence exists, is authentic, or is within a suspect's [*8] control. *Doe v. United States, 487 U.S. 201, 209, 108 S. Ct. 2341, 101 L. Ed. 2d 184 (1988)* [hereinafter *Doe II*]. The privi-

lege against self-incrimination protects a suspect from being compelled to disclose any knowledge he has, or to speak his guilt. *Id. at 210-11.* The suspect may not be put in the "cruel trilemma" of choosing between self-accusation, perjury, or contempt. *Id. at 212.*

The government points to *Doe II* in support of its contention that entering the password is non-testimonial and therefore not privileged. In *Doe II,* a suspect was subpoenaed to sign a form requesting his bank records from banks in the Cayman Islands and Bermuda. *Id. at 203.* The suspect asserted his privilege against self-incrimination, arguing that signing the form would be testimonial and incriminating. *Id. at 207-09.* But the form only spoke in the hypothetical, not referencing specific accounts or banks. *Id. at 215.* The Court held that the form did not acknowledge any accounts and made no statement, implicitly or explicitly, about the existence or control over any accounts. *Id. at 215-16.* Because signing the form made no statement about the suspect's knowledge, the Court held that the act lacked testimonial significance and the privilege [*9] did not apply. *Id. at 218.*

Entering a password into the computer implicitly communicates facts. By entering the password Boucher would be disclosing the fact that he knows the password and has control over the files on drive Z. The procedure is equivalent to asking Boucher, "Do you know the password to the laptop?" If Boucher does know the password, he would be faced with the forbidden trilemma; incriminate himself, lie under oath, or find himself in contempt of court. *Id. at 212.*

Unlike the situation in *Doe II,* Boucher would be compelled to produce his thoughts and the contents of his mind. In *Doe II,* the suspect was compelled to act to obtain access without indicating that he believed himself to have access. Here, when Boucher enters a password he indicates that he believes he has access.

The Supreme Court has held some acts of production are unprivileged such as providing fingerprints, blood samples, or voice recordings. *Id. at 210.* Production of such evidence gives no indication of a person's thoughts or knowledge because it is undeniable that a person possesses his own fingerprints, blood, and voice. *Id. at 210-11.* Unlike the unprivileged production of such samples, it is not without [*10] question that Boucher possesses the password or has access to the files.

In distinguishing testimonial from non-testimonial acts, the Supreme Court has compared revealing the combination to a wall safe to surrendering the key to a strongbox. *See id. at 210, n.9*; *see also United States v. Hubbell, 530 U.S. 27, 43, 120 S. Ct. 2037, 147 L. Ed. 2d 24 (2000).* The combination conveys the contents of one's mind; the key does not and is therefore not testimonial. [1] *Doe II, 487 U.S. at 210, n.9.* A password, like a combination, is in the suspect's mind, and is therefore testimonial and beyond the reach of the grand jury subpoena.

1 The Supreme Court's use of the term "surrender" creates a reasonable inference that the Court assumed the government's prior knowledge of the suspect's possession of the key. If it was unknown whether the suspect had the key, compelling the production of the key would disclose the suspect's access to the strongbox contents and might therefore be a privileged testimonial act.

II. Effect of Non-Viewing

The government has offered to restrict the entering of the password so that no one views or records the password. While this would prevent the government from knowing what the password is, it would not change [*11] the testimonial significance of the act of entering

the password. Boucher would still be implicitly indicating that he knows the password and that he has access to the files. The contents of Boucher's mind would still be displayed, and therefore the testimonial nature does not change merely because no one else will discover the password.

III. Effect of Exclusion from Evidence

During the hearing on the motion, the government offered not to use the production of the password against Boucher. The government argues that this would remove the testimonial aspect from the act, and that the act would therefore be unprivileged. This is the same argument the Supreme Court rejected in *United States v. Hubbell, 530 U.S. 27, 120 S. Ct. 2037, 147 L. Ed. 2d 24 (2000)*.

In *Hubbell,* the Court determined the precise scope of a grant of immunity with respect to the production of subpoenaed documents. *Id. at 34*. The government subpoenaed business documents from Hubbell but granted him immunity for the production. *Id. at 31*. The government then prosecuted him for fraud based on the documents that he had produced. *Id.* The government argued that it was not making improper use of the production because it did not need the act of production itself [*12] as evidence and the documents themselves were unprivileged. *Id. at 40-45*. The government argued that the immunity granted did not preclude "derivative use", use of the fruits of the production, because the documents themselves were the fruit only of the simple physical act of production. *Id. at 43*.

The Court acknowledged that the government would not have to use the act of production as evidence to prove the existence, authenticity, or custody of the documents, or to prove the charges against Hubbell. *Id. at 41*. However, the Court noted that Hubbell's immunity needed to extend to any derivative use in order to protect his *Fifth Amendment* privilege. *Hubbell, 530 U.S. at 38-39* (citing *Kastigar v. United States, 406 U.S. 441, 92 S. Ct. 1653, 32 L. Ed. 2d 212 (1972))*. The Court also re-emphasized the critical importance of a suspect's protection from prosecution based on sources of information obtained from compelled testimony. *Id. at 39*.

The Court found that the act of production had testimonial aspects, because production communicated information about the existence, custody, and authenticity of the documents. *Id. 36-37*. The compelled testimony of the production became the first in a chain of evidence which led to the [*13] prosecution. *Id. at 42*. The Court refused to divorce the physical act of production from its implicit testimonial aspect to make it a legitimate, wholly independent source. *Id. at 40*. In doing so, the Court reaffirmed its holding that derivative use immunity is coextensive with the privilege against self-incrimination. *Id. at 45*. Accordingly, the Court held that Hubbell could not be prosecuted based on the documents and only evidence wholly independent of the production could be used. *Id. at 45-46*.

Here, as in *Hubbell,* the government cannot separate the non-testimonial aspect of the act of production, entering the password, from its testimonial aspect. The testimonial aspect of the entry of the password precludes the use of the files themselves as derivative of the compelled testimony. Any files the government would find based on Boucher's entry of the password could not be used against him, just as Hubbell's documents could not be used against him. Barring the use of the entry of the password is not enough to protect Boucher's privilege.

IV. Foregone Conclusion

The government also asserts that the information gained through entry of the password is a "foregone conclusion", therefore [*14] no privilege applies. The Government relies on *In re Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992, 1 F.3d 87 (2d Cir. 1993)* [hereinafter *Doe III*]. *Doe III* held that the privilege

against self-incrimination does not apply to an act of production if the existence and location of the subpoenaed evidence is known to the government and the production would not "implicitly authenticate" the evidence. *Id. at 93.*

In *Doe III,* the suspect had produced a photocopy of a personal calendar but the Government suspected that the calendar had been altered through the whiting out of incriminating entries. *Id. at 88-90.* The government subpoenaed the suspect to produce the original calendar before the grand jury. *Id.* The Second Circuit reasoned that the existence and location of the calendar was a "foregone conclusion" because it was known, through production of the photocopy, that the suspect had possession of the calendar and the original calendar added little or nothing to the sum total of the government's information. *Id. at 93.* The court also found that act of production itself was not necessary to authenticate the original calendar because the Government could authenticate it simply by comparing [*15] it to the photocopy. *Id.* Therefore, because the government had knowledge of the existence and location of the original calendar and did not need to use the act of production to authenticate the original calendar, the suspect had no act of production privilege and was required to produce the original calendar before the grand jury. *Id. at 93-94.*

Here, the subpoena can be viewed as either compelling the production of the password itself or compelling the production of the files on drive Z. Both alternatives are distinguishable from *Doe III.*

If the subpoena is requesting production of the files in drive Z, the foregone conclusion doctrine does not apply. While the government has seen some of the files on drive Z, it has not viewed all or even most of them. While the government may know of the existence and location of the files it has previously viewed, it does not know of the existence of other files on drive Z that may contain incriminating material. By compelling entry of the password the government would be compelling production of all the files on drive Z, both known and unknown. Unlike in *Doe III,* the files the government has not seen could add much to the sum total of the government's [*16] information. Therefore, the foregone conclusion doctrine does not apply and the act of production privilege remains.

Since the government is trying to compel the production of the password itself, the foregone conclusion doctrine cannot apply. The password is not a physical thing. If Boucher knows the password, it only exists in his mind. This information is unlike a document, to which the foregone conclusion doctrine usually applies, and unlike any physical evidence the government could already know of. It is pure testimonial production rather than physical evidence having testimonial aspects. Compelling Boucher to produce the password compels him to display the contents of his mind to incriminate himself. *Doe III* did not deal with production of a suspect's thoughts and memories but only previously created documents. The foregone conclusion doctrine does not apply to the production of non-physical evidence, existing only in a suspect's mind where the act of production can be used against him.

Conclusion

For the foregoing reasons, the motion to quash the subpoena is GRANTED.

Dated at Burlington, in the District of Vermont, this 29th day of November, 2007.

/S/ Jerome J. Niedermeier

Jerome [*17] J. Niedermeier

United States Magistrate Judge

Any party may object to this Report and Recommendation within 10 days after service by filing with the clerk of the court and serving on the magistrate judge and all parties, written objections which shall specifically identify the

portions of the proposed findings, recommendations or report to which objection is made and the basis for such objections. Failure to file objections within the specified time waives the right to appeal the District Court's order. *See* Local Rules 72.1, 72.3, 73.1; *28 U.S.C. § 636(b)(1)* ; *Fed. R. Civ. P. 72(b)*, *6(a)* and *6(e)*.

LexisNexis®

In re: GRAND JURY SUBPOENA TO SEBASTIEN BOUCHER

No. 2:06-mj-91

UNITED STATES DISTRICT COURT FOR THE DISTRICT OF VERMONT

2009 U.S. Dist. LEXIS 13006

February 19, 2009, Decided
February 19, 2009, Filed

PRIOR HISTORY: *In re Grand Jury Subpoena (Boucher), 2007 U.S. Dist. LEXIS 87951 (D. Vt., Nov. 29, 2007)*

DISPOSITION: Motion to quash denied.

COUNSEL: [*1] For Sebastien D. Boucher, Defendant (1): Bradley S. Stetler, Esq., LEAD ATTORNEY, Stetler, Allen & Kampmann, Burlington, VT; James H. Budreau, LEAD ATTORNEY, Law Office of James Budreau, Boston, MA.

For USA, Plaintiff: Timothy C. Doherty, Jr., AUSA, LEAD ATTORNEY, United States Attorney's Office, District of Vermont, Burlington, VT.

JUDGES: William K. Sessions III, Chief Judge, U.S. District Judge.

OPINION BY: William K. Sessions III

OPINION

MEMORANDUM of DECISION

The Government appeals the United States Magistrate Judge's Opinion and Order (Doc. 35) granting defendant Sebastien Boucher's motion to quash a grand jury subpoena on the grounds that it violates his *Fifth Amendment* right against self-incrimination. The grand jury subpoena directs Boucher to

> provide all documents, whether in electronic or paper form, reflecting any passwords used or associated with the Alienware Notebook Computer, Model D9T, Serial No. NKD900TA5L00859, seized from Sebastien Boucher at the Port of Entry at Derby Line, Vermont on December 17, 2006.

In its submission on appeal, the Government stated that it does not in fact seek the password for the encrypted hard drive, but requires Boucher to produce the contents of his encrypted hard drive [*2] in an unencrypted format by opening the drive before the grand jury. (Gov't's Appeal 2.) In oral argument and post-argument submissions, the Government

stated that it intends only to require Boucher to provide an unencrypted version of the drive to the grand jury. (Hr'g Tr. 6, Apr. 30, 2008.)

I. Procedural History, Jurisdiction and Standard of Review

The Government filed a criminal complaint against Boucher on December 18, 2006, alleging that he knowingly transported child pornography in interstate or foreign commerce in violation of *18 U.S.C. § 2252A(a)(1)*. It applied for and was granted a search warrant for the contents of a laptop computer that was seized from Boucher's vehicle at the Derby Line Port of Entry on December 17, 2006. The Government's forensic expert was unable to conduct a search of the computer's contents because the contents were password-protected. The grand jury issued a subpoena to Boucher for any passwords associated with the laptop. Boucher moved to quash the subpoena, arguing that the act of production of this information would violate his *Fifth Amendment* privilege against self-incrimination.

The United States Magistrate Judge conducted evidentiary hearings on [*3] the motion to quash on July 9 and November 1, 2007, and issued an opinion and order granting the motion on November 29, 2007. [1] On January 2, 2008, the Government filed an appeal of the Magistrate Judge's decision with this Court, which heard argument on April 30, 2008.

> 1 The Government has suggested that the United States Magistrate Judge was not "the appropriate arbiter of [Boucher's] *Fifth Amendment* claim." (Gov't's Resp. 2 (Doc. 57).) As far as the Court is aware, the Government did not object to this manner of proceeding prior to receiving an unfavorable ruling from the Magistrate Judge.

The United States Magistrate Judge was authorized to hear and determine this matter pursuant to his "additional duties" jurisdiction under *28 U.S.C. § 636(b)(3)*. Review under this subsection of the Federal Magistrates Act is de novo. *See Peretz v. United States, 501 U.S. 923, 939, 111 S. Ct. 2661, 115 L. Ed. 2d 808 (1991)* (de novo review appropriate for *§ 636(b)(3)* referral when requested); *Mathews v. Weber, 423 U.S. 261, 270, 96 S. Ct. 549, 46 L. Ed. 2d 483 (1976)* (Congress intended that district judge retain ultimate responsibility for decision making when a magistrate judge exercises additional duties jurisdiction).

II. Factual Background

The material facts pertaining [*4] to the motion to quash, as set forth in the Magistrate Judge's Opinion and Order, have not been disputed. On December 17, 2006, Boucher and his father crossed the Canadian border into the United States at Derby Line, Vermont. A Custom and Border Protection inspector directed Boucher's car into secondary inspection. The inspector conducting the secondary inspection observed a laptop computer in the back seat of Boucher's car, which Boucher acknowledged as his. The inspector searched the computer files and found approximately 40,000 images.

Based upon the file names, some of the files appeared to contain pornographic images, including child pornography. The inspector called in a Special Agent for Immigration and Customs Enforcement ("ICE") with experience and training in recognizing child pornography. The agent examined the computer and file names and observed several images of adult pornography and animated child pornography. He clicked on a file labeled "2yo getting raped during diaper change," but was unable to open it. The "Properties" feature indicated that the file had last been opened on December 11, 2006.

After giving Boucher *Miranda* warnings, and obtaining a waiver from him, the [*5] agent asked Boucher about the inaccessible file. Boucher replied that he downloads many pornographic files from online newsgroups onto a

desktop computer and transfers them to his laptop. He stated that he sometimes unknowingly downloads images that contain child pornography, but deletes them when he realizes their contents.

The agent asked Boucher to show him the files he downloads. Boucher navigated to drive "Z" of the laptop, and the agent began searching the Z drive. The agent located and examined several videos or images that appeared to meet the definition of child pornography.

The agent arrested Boucher, seized the laptop and shut it down. He applied for and obtained a search warrant for the laptop. In the course of creating a mirror image of the contents of the laptop, however, the government discovered that it could not find or open the Z drive because it is protected by encryption algorithms from the computer software "Pretty Good Protection," which requires a password to obtain access. The government is not able to open the encrypted files without knowing the password. In order to gain access to the Z drive, the government is using an automated system which attempts to guess [*6] the password, a process that could take years.

The grand jury subpoena directed Boucher to produce the password. The request described in the original subpoena, and the request to which the magistrate judge directed his attention, have been narrowed to requiring Boucher to produce an unencrypted version of the Z drive. (Gov't's Resp. 3 (Doc. 57).)

III. Discussion

The *Fifth Amendment to the United States Constitution* protects "a person . . . against being incriminated by his own compelled testimonial communications." *Fisher v. United States, 425 U.S. 391, 409, 96 S. Ct. 1569, 48 L. Ed. 2d 39 (1976)*. There is no question that the contents of the laptop were voluntarily prepared or compiled and are not testimonial, and therefore do not enjoy *Fifth Amendment* protection. *See id. at 409-10*; *accord United States v. Doe, 465 U.S. 605, 611-12, 104 S. Ct. 1237, 79 L. Ed. 2d 552 (1984)* ("*Doe I*").

"Although the contents of a document may not be privileged, the act of producing the document may be." *Id. at 612*. "'The act of production' itself may implicitly communicate 'statements of fact.' By 'producing documents in compliance with a subpoena, the witness would admit that the papers existed, were in his possession or control, and were authentic.'" *United States v. Hubbell, 530 U.S. 27, 36, 120 S. Ct. 2037, 147 L. Ed. 2d 24 (2000)* [*7] (quoting *Doe v. United States, 487 U.S. 201, 209, 108 S. Ct. 2341, 101 L. Ed. 2d 184 (1988)* ("*Doe II*")). Thus, "the *Fifth Amendment* applies to acts that imply assertions of fact." *Doe II, 487 U.S. at 209*. It is "the attempt to force [an accused] to 'disclose the contents of his own mind' that implicates the *Self-Incrimination Clause*." *Id. at 211* (quoting *Curcio v. United States, 354 U.S. 118, 128, 77 S. Ct. 1145, 1 L. Ed. 2d 1225 (1957))*. Moreover, "[c]ompelled testimony that communicates information that may 'lead to incriminating evidence' is privileged even if the information itself is not inculpatory." *Hubbell, 530 U.S. at 38* (quoting *Doe II, 487 U.S. at 208, n.6*).

At issue is whether requiring Boucher to produce an unencrypted version of his laptop's Z drive would constitute compelled testimonial communication. *See In re Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992 (United States v. Doe), 1 F.3d 87, 93 (2d Cir. 1993)* ("Self-incrimination analysis now focuses on whether the creation of the thing demanded was compelled and, if not, whether the act of producing it would constitute compelled testimonial communication . . . regardless of 'the contents or nature of the thing demanded.'") (quoting *Baltimore Dep't of Soc. Servs. v. Bouknight, 493 U.S. 549, 555, 110 S. Ct. 900, 107 L. Ed. 2d 992 (1990)* [*8] (O'Connor, J., concurring)).

The act of producing documents in response to a subpoena may communicate incriminating facts "in two situations: (1) 'if the existence and location of the subpoenaed papers are unknown to the government'; or (2) where production would 'implicitly authenticate' the documents." *Id.* (quoting *United States v. Fox, 721 F.2d 32, 36 (2d Cir. 1983))*.

Where the existence and location of the documents are known to the government, "no constitutional rights are touched," because these matters are a "foregone conclusion." *Fisher, 425 U.S. at 411*. The Magistrate Judge determined that the foregone conclusion rationale did not apply, because the government has not viewed most of the files on the Z drive, and therefore does not know whether most of the files on the Z drive contain incriminating material. Second Circuit precedent, however, does not require that the government be aware of the incriminatory *contents* of the files; it requires the government to demonstrate "with reasonable particularity that it knows of the existence and location of subpoenaed documents." *In re Grand Jury Subpoena, 1 F.3d at 93*.

Thus, where the government, in possession of a photocopy of a grand [*9] jury target's daily calendar, moved to compel compliance with a subpoena for the original, the Second Circuit ruled that no act of production privilege applied. *Id. at 93-94*. The existence and location of the calendar were foregone conclusions, because the target had produced a copy of the calendar and testified about his possession and use of it. *Id. at 93*.

The target's production of the original calendar was also not necessary to authenticate it; the government could authenticate the calendar by establishing the target's prior production of the copy and allowing the trier of fact to compare the two. *Id.*

Boucher accessed the Z drive of his laptop at the ICE agent's request. The ICE agent viewed the contents of some of the Z drive's files, and ascertained that they may consist of images or videos of child pornography. The Government thus knows of the existence and location of the Z drive and its files. Again providing access to the unencrypted Z drive "adds little or nothing to the sum total of the Government's information" about the existence and location of files that may contain incriminating information. *Fisher, 425 U.S. at 411*.

Boucher's act of producing an unencrypted version of [*10] the Z drive likewise is not necessary to authenticate it. He has already admitted to possession of the computer, and provided the Government with access to the Z drive. The Government has submitted that it can link Boucher with the files on his computer without making use of his production of an unencrypted version of the Z drive, and that it will not use his act of production as evidence of authentication. (Hr'g Tr. 38, 39, 41.) [2]

> 2 By accepting the Government's submission on this point, the Court makes no ruling on whether the Government can in fact authenticate the unencrypted Z drive or its contents, including images not viewed by the ICE agent during the initial search.

Because Boucher has no act of production privilege to refuse to provide the grand jury with an unencrypted version of the Z drive of his computer, his motion to quash the subpoena (as modified by the Government) is **denied.** Boucher is directed to provide an unencrypted version of the Z drive viewed by the ICE agent. The Government may not make use of Boucher's act of production to authenticate the unencrypted Z drive or its contents either before the grand jury or a petit jury. The Government's appeal of the Magistrate [*11] Judge's opinion and order (Doc. 35) is sustained.

Dated at Burlington, Vermont this 19th day of February, 2009.

/s/ William K. Sessions III
William K. Sessions III

Chief Judge, U.S. District Court

LexisNexis®

UNITED STATES OF AMERICA, v. ABRAHAM PEARSON, Defendant.

1:04-CR-340

UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF NEW YORK

2006 U.S. Dist. LEXIS 32982

May 24, 2006, Decided

COUNSEL: [*1] Terence L. Kindlon, Esq., Kindlon and Shanks, P.C., Albany, NY.

Thomas Spina Jr., Esq., Assistant United States Attorney, Glenn T. Suddaby, United States Attorneys Office, Albany, NY.

JUDGES: Thomas J. McAvoy, Senior, U.S. District Judge.

OPINION BY: Thomas J. McAvoy

OPINION

MEMORANDUM

DECISION and ORDER

I. INTRODUCTION

Defendant is charged in a multi-count Second Superseding Indictment with violations of Title *18, United States Code, Sections 2251(a)* [Production of Child Pornography], *2252A(a)(1)* [Distribution of Child Pornography], *2252A(a)(2)*[Receipt of Child Pornography], *2252A(a)(5)(B)* [Possession of Child Pornography], and *2257* [Failure to Maintain Records]. Before the Court is Defendant's second omnibus motion [1] seeking (1) the dismissal of the Second Superceding Indictment based upon an alleged violation of the defendant's attorney-client privilege and destruction of exculpatory material, (2) the dismissal of counts 67-73 as multiplicitous, (3) the dismissal of counts 1-66 of the Second Superceding Indictment as legally insufficient under the *Commerce Clause*, (4) the suppression of physical evidence seized as a result of a search [*2] warrant executed on December 1, 2005, (5) the return of all property seized on December 1, 2005, (6) discovery, (7) the identification of all prior bad acts of Defendant, and (8) leave to make additional motions.

1 Defendant previously brought an Omnibus Motion. In a Memorandum-Decision and Order dated November 3, 2005, the Court ruled that Defendant's motion seeking: (1) dismissal of Counts 67, 69, and 70 as multiplicitous of Counts 1-66 and 68 was denied without prejudice to renewal at trial; (2) dismissal of Counts 1-66 as legally insufficient under the *Commerce Clause*

was denied; (3) suppression of all physical evidence obtained as a result of a search warrant was denied; (4) in the alternative to suppression, an evidentiary hearing pursuant to *Franks v. Delaware, 438 U.S. 154, 98 S. Ct. 2674, 57 L. Ed. 2d 667 (1978)*, was denied; (5) discovery pursuant to *Rule 16 of the Federal Rules of Criminal Procedure* was denied; (6) production of all Brady material was denied; (7) early production of Jencks material was denied; (8) identification of all prior bad acts of defendant the government intends to introduce at trial was denied; (9) preservation of law enforcement notes was denied; and (10) permission to make further motions was denied with the exception that "Defendant will be permitted to make additional motions only for good cause shown should additional discovery produce new material facts and issues."

[*3] In addition, Defendant brings a separate motion seeking to quash a subpoena served upon him that requires him to produce at his trial "any and all passwords, keys, and/or log-ins used to encrypt any and all files" recovered on the computer drives and disks taken from his residence pursuant to a search warrant executed on December 1, 2005.

The Court will address these arguments seriatim.

II. BACKGROUND

On June 13, 2003, Jane Doe # 2, then a 15-year-old female, informed members of the Niskayuna Police Department (NPD) that Defendant was producing child pornography involving Jane Doe # 2 and Jane Doe # 1, then a 17-year-old female. Fallon Aff. P3. In this regard, Jane Doe # 2 asserted that she and the other minor were paid to perform sexual acts with Defendant while he was filming them in his home at 2065 Orchard Park Drive, Niskayuna, New York. Id. The NPD obtained a New York State warrant to search Defendant's home and executed it on June 13, 2003. Id. Numerous items of evidence were seized, including computers, computer hard drives, and computer disks. Id. The computer disks allegedly contained hours of videos and still images of Defendant and Jane Does # [*4] 1 and/or # 2 engaged in sexually explicit conduct. Id. Shortly after this discovery, the FBI became involved in the investigation. The investigation revealed that Defendant had labeled the disks in detailed fashion by date, volume, length, camera used, individuals appearing, and type of sexual activity. Id. P4. The FBI determined that on some disks or files, the individuals appearing in the videos and photographs were identified by code names. For instance, according to the Government the two Jane Does were, in some instances, both referred to as "SITGAL" ("Sitgal # 1" and "Sitgal # 2") because both had been employed as babysitters for Defendant's children. Defendant referred to himself as "Ov" based upon his Hebrew name. Id. PP4, 10(A).

The FBI also learned that Defendant sent, via the Internet, numerous images and movie files of Jane Does # 1 & # 2 engaged in sexually explicit conduct to David Gilinsky, Defendant's long-time friend who lived in Cleveland, Ohio. Id. P5. Gilinsky was interviewed and voluntarily turned over his computer to the FBI for analysis. Id. Sexually explicit images of Jane Doe # 1 were recovered from his computer. Id. Gilinsky also stated [*5] to the FBI that Pearson sent him numerous computer files from NY to Ohio via the Internet, and that the files contained sexually explicit images of Jane Does # 1 & # 2. Id. Gilinsky asserted that Defendant told him that the girls were 17 years old. Id. Gilinsky later testified before a federal grand jury that returned a Superceding Indictment and a Second Superceding Indictment (discussed below). Id.

On February 16, 2004, Elijah Pearson, Defendant's father and an attorney admitted to practice law in the State of New York, wrote a

letter to Glenn Suddaby, United States Attorney for the Northern District of New York. The letter appears to be a personal appeal to Suddaby regarding the prosecution of Defendant and includes the following passage: "I do not ask you for any favor. I do not participate or advise [Defendant]. He has a very good lawyer." Govt. Attach. G. At no time has Elijah Pearson entered an appearance in this case and, as early as the initial appearance on July 7, 2004, Defendant has indicated that he was represented by his current attorney-of- record, Terence L. Kindlon, Esq. See dkt. # 3.

On June 30, 2004, Defendant was indicted by a federal grand jury [*6] on one count of producing pornography based upon his alleged activities with Jane Doe # 1. He was arrested on July 6, 2004, and released on bail. Upon his release, Defendant began residing at 4635 Slippery Rock Circle, Manlius, New York with his father, Elijah Pearson. Fallon Aff. PP6-7. On February 11, 2005, Defendant was charged in a 71 Count Superseding Indictment with the production, transportation, possession, and receipt of child pornography, and with failing to keep individually identifiable records in violation of *18 U.S.C. §§ 2251(a), 2251(d), 2256(8), 2252A(a)(1), 2252A(a)(2), 2252(a)(5)(B)*, and *2257*.

On November 29, 2005, the FBI received the results of a computer forensic examination conducted on the computer surrendered by Gilinsky. Fallon P8. The Government contends that this revealed that on multiple occasions between February 27, 2003 and May 27, 2003, Defendant sent Gilinsky numerous sexually explicit images of Jane Doe # 1, as well as numerous e-mail messages. Id. During these exchanges, Defendant purportedly [*7] used one of two America Online email addresses - "Peall2065" and "Elijah1926." Id. America Online records showed that the "Peall2065" address was registered to Defendant, and the "Elijah1926" address was registered to Defendant's father. Id. P9.

Review of the email messages sent between Defendant and Gilinsky led the Government to believe that Gilinsky provided Defendant with sexually explicit images of Jane Does # 1 & # 2 after Defendant's home was searched and after he was arrested in June 2003. Id. P10. In addition, in an e-mail dated March 11, 2004 from "Peall2065" to Gilinsky's e-mail account, Peall2065 wrote:

> To finish this morning's conversation: Ov will havem [sic] notebook at Binghamton meeting. Audio clips for analysis & manipulation could be crucial to Ov's defense. Remember SitGal # 2 is not legal. Ov has a "safe" for securing data & will change his password then so that no computer or human can retrieve saved data. The thing encrypts immediately (live/realtime) and will have a password like: eolKleGH93*vfOY3Gw4kn&jd . Also a shredder delete program is included to properly delete files &/or "free space". . . .

Id. P10(C).

The Government [*8] believed that this last e-mail indicated that Defendant was going to try to manufacture evidence that might exonerate him on the various charges, perhaps creating an audio or video file in which it appeared that the Jane Does represented that they were 18 years of age or older. Id. P18(b).

On November 20, 2005, the Government applied for a search warrant of Defendant's residence that he shared with his father, and of the computers in the residence, on the belief that Defendant had reacquired sexually explicit images of Jane Does # 1 & # 2. Id. P11. The warrant application was granted, authorizing the seizure of computers and computer related

media that might divulge evidence of the production, possession, receipt and distribution of visual depictions of minors engaged in sexually explicit conduct, including evidence of communications between Defendant, a.k.a. "Ov", "Peall2065@aol.com", or "Elijah1926@aol.com, and Gilinsky (a.k.a. "dOv") at his America On Line account. Id.

The warrant was executed on December 1, 2005. Id. P12. At the time the warrant was executed, Defendant and his father were present. Id. PP40-41. The Government contends that at no time [*9] did Elijah Pearson or Defendant represent that Elijah Pearson was representing Defendant, nor did government agents or attorneys have knowledge to that effect. Id. PP36, 40-41; see Spina Aff. P29. Defendant has not presented any competent evidence to the contrary. The Government also contends that "at no time [on December 1, 2005] did Elijah Pearson or the defendant indicate that there were attorney-client materials or other privileged communications on either of the computers." Fallon Aff. P41. The Government concedes, however, that Defendant and his father represented to Government agents that Defendant used "his computer to research his case," and that "there would be research for other unrelated legal matters [of the father] on the computers." Id.

Pursuant to the search warrant, the Government seized, *inter alia,* (1) a 400 GB Sony Vaio Computer, Model PCV 1152, s/n 3000001; (2) a Sony Vaio Computer, model PCV-RX5500, s/n A8023273A 0204338; (3) a Western Digital external hard drive, s/n WCAEK1534T54; (4) a Sony thumb drive; (5) a Lexor thumb drive; and (6) over one hundred computer disks. Id. P12.

> Other than the computer disks, this evidence was [*10] logged into evidence for analysis by a Computer Analysis Response Team (CART) agent, specifically trained in forensically analyzing computer media. Prior to analyzing any of the computer and computer media, mirror images were made.

Id. P13.

On Friday, December 2, 2005, the CART agent searched the computer media using the victims and Gilinsky's names. He recovered and printed out a multi-page typed document that he believed contained admissions by Defendant, and placed the document on Case Agent Fallon's desk. Id. P14. Fallon reviewed the document on the following Monday, December 5, 2005. Id. The CART agent was not in the office during the week of December 5, 2005 so Fallon could not ask where or in what file the document was found. Id. However, based upon review of the document, Fallon concluded that the document consisted of notes by Defendant about his case and contained what appeared to be an admission that he still possessed a computer disk containing sexually explicit images of the minors. Id.

Fallon also conducted his own search of the computer disks during the week of December 5, 2005 and discovered the following which he believed were relevant [*11] to the instant case:

(a) Four recorded telephone conversations between Defendant and Gilinsky. Each file had a ".wmv" extension, which led Fallon to believe that they were files similar to the sexually explicit images found on Gilinsky's computer (that were purportedly sent by Defendant), and included the name "Gilinsky" in the file name. Id. P15(a);

(b) Sixteen video files, two of which depicted unknown women stating that they were "18" and "18 and 1/2", respectively. Id. P15(b). Each file contained the ".wmv" extension, and were recovered from a disk labeled "BU Drive Easy Pass (X:) Case & Vid Editing Parts." Id.

These were contained in a folder named "PRIVATE- For my Attorney-imp case files" and in subfolders named "ImpCaseData.." Id. Fallon contends that he did not review the contents of any of the files in this folder except for the files that were identifiable as video folders by their size and ".wvm" extension. Id. Upon reviewing the two videos of the women stating their ages, Fallon formed the opinion that they "were evidence of the defendant attempting to obstruct justice by manipulating the audio portions of the sexually explicit video tapes he has reacquired [*12] [from Gilinsky]." Id.

(c) A one page document containing two emails from Elijah Pearson to Gilinsky. Id. P15(c). In one email, a copy of which had already been recovered from Gilinsky's computer, Elijah Pearson instructs Glinsky to erase evidence and discusses a possible interview with FBI agents. Id. The second e-mail also discusses a possible interview with FBI agents. The document was recovered from a disk labeled "Case B.U. 11-20-04", found in a file named "PRIVATE-For my Attorney-imp case files" and in a subfolder entitled "Dov Warning before FBI." Id. The file was named "emailfromEAPbeforedovFBIMeeting.jpg." Id. Special Agent Fallon "believed it was appropriate to view this file since it appeared to be a communication with Gilinsky, which was covered by the terms of the search warrant." Id.

The FBI also conducted a "limited forensic examination" of the 400 GB Sony Vaio Computer, Model PCV 1152, s/n 3000001. Id. P16. The "user" of the computer is identified in the computer's registry as "CaptainOv," leading the FBI to conclude that Defendant was the user since he had referred to himself as "the Captain" and "Ov." Three image files were recovered [*13] from the computer depicting what appeared to the FBI to be images of the minor victims albeit not sexually explicit. Id. The FBI also found a number of encrypted files within a file labeled "steganosencryptionsafes," but did not review any text files from this computer. Id.

A "very limited forensic examination" of the Sony Vaio Computer, model PCV-RX5500, s/n A8023273A 0204338 divulged (1) a file named "C:/Documents and Settings/HutUsers/Desktop/Excellent-FakeIDs ([Jane Doe # 2]).htm"; and (2) an email dated March 18, 2004, from "steganos.asknet.de" to "Peall20056@aol.com" in which "a password and serial number necessary for downloading software capable of encrypting files were provided." Id. P17. The content of text documents from the computer were not reviewed, and the items recovered were not in files indicating that they may be privileged information. Id.

A forensic examination of the Western Digital hard drive revealed a "2.3 gigabyte encrypted folder/container." Id. P18. Special Agent Fallon asserts "[a] file this size is large enough to contain a number of movie files and still images." Id. However, the FBI is unable, at this time, to access [*14] the file to determine whether it contains any sexually explicit images of the minor. Id. The Western Digital hard drive did contain "files whose names appear to indicate that they contain privileged material" so these files were not reviewed. Id.

The Court's file contains a letter written by Elijah A. Pearson to United States Magistrate Judge Randolph F. Treece. The letter is dated December 2, 2005 and was purportedly carbon copied to "Special Agent David Fallon; Judge Norman Mordue; Terrence Kindlon, Esq.; Thomas Spina, USA; and Rebecca Doyle, Pretrial Services." The letter, which is stamped "received" by Judge Mordue's Chambers on December 6, 2005, states in relevant part:

> I was the subject of a search warrant on December 1, 2005. Both my computers were taken together with other materials.
>
> I am an attorney working on my son's case upon the computers which contained work product in his case and other legal matters.

> I strongly believe the search was illegal and improper. It was an improper use of search and seizure of my legal material. Original exculpatory evidence was seized making a fair trial impossible at this point for defendant Abraham Pearson. All [*15] of the defense case strategy and information, totaling over 10 gigabytes of computer space, was taken....

The FBI believed that encrypted folders and files found on the various computers and computer media might have contained sexually explicit images of the minor victims. Id. P19. Therefore, on December 7, 2004 the FBI sent the following items to the FBI's Cryptological and Electronic Analysis Unit: (1) a mirror image of the 400 GB Sony Vaio; (2) a mirror image of the Western Digital Hard Drive; (3) the Sony thumb drive; and (4) a computer disk labeled "Archive & B.U. 8/04" and which purportedly indicated that "it contains a long Steganos password." Id. The Cryptological and Electronic Analysis Unit has been instructed to try to access any encrypted files to determine whether they contain sexually explicit images of the minor victims, but not to view any text documents or potentially privileged material. Id.

On December 12, 2005, Special Agent Fallon met with Assistant United States Attorney Thomas Spina. Id. P20; Spina Aff. P11. Fallon advised Spina of the various items that had been recovered from the computer thumb drive and the computer disks. Fallon Aff. [*16] P21; Spina Aff. P11. The first item presented to Spina was the multi-page typed document that Fallon believed contained an admission by Defendant that he still possessed computer disks containing sexually explicit images of one of the minor victims. Fallon Aff. P22; Spina Aff. P12; Govt. Ex. H. Spina noticed that the document "contained notes apparently written by the defendant about materials that could be used to impeach various witnesses and some legal research." Spina Aff. P12. [2] Upon reviewing the document, Spina inquired of Fallon regarding the source of the document. Fallon Aff. P22; Spina Aff. P12. Fallon purportedly responded that it was found on a thumb drive after a search for the name of the minor victims and the name "Gilinsky," but that he did not know the exact source and would check with the CART agent and advise by the end of the day. Fallon Aff. P22; Spina Aff. P12. Spina also was advised of or reviewed other potentially relevant information as follows: (a) recorded telephone conversations between Defendant and Gilinsky, Spina Aff. P13; (b) the video files of the two unknown women stating that they are 18 and 18 1/2, id. P14; (c) the two emails from Elijah Pearson [*17] to Gilinsky, id. P15; and (d) the file named "C:/Documents and Settings/HutUsers/Desktop/Excellent-FakeIDs ([Jane Doe # 2]).htm"; and the email dated March 18, 2004, from "steganos.asknet.de" to "Peall20056@aol.com" in which a password and serial number necessary for downloading software capable of encrypting files were provided. Id. P16.

> 2 Spina provides a footnote in his affidavit indicating that the impeachment information in the document was already known to the Government. See Spina Aff. P12, n. 1.

Later in the day on December 12, 2005, Special Agent Fallon advised AUSA Spina that the document containing what appears to be Defendant's notes and the document containing e-mails from Elijah Person were "in folders whose names indicated that they may be privileged documents." Id. P18. He indicated further, however, that the recorded telephone calls were from a separate computer disk which "was not labeled in the manner that would indicate that they were privileged." Id. AUSA Spina [*18] sealed the document containing

Defendant's notes, instructed Fallon not to access any text documents on the computer media, and requested the FBI to create a "taint" team before conducting any further searches. Id. P20. Later that day, Spina advised Fallon "that the taint team should not view any materials seized on December 1, 2005, and that there should be no additional searches of the media." Id. FBI's Cryptological and Electronic Analysis Unit is still attempting to access encrypted files in order to determine whether they contain sexually explicit images of the victims, but have been instructed not to view "any text documents or potentially privileged material." Id. P21.

The Government contends that:

> Other than any sexually explicit images of the minors possibly contained in encrypted files and the videos contained in the "Case18Clips" folder, the government does not intend to introduce any evidence recovered during the December 1, 2005, search at trial.

Id. P21.

On December 14, 2005, the Government re-interviewed David Gilinsky prior to his grand jury testimony that day. Id. P23; Gilinsky Aff. P10. Gilinsky's attorney was present during the [*19] meeting. Gilinsky Aff. P10. Spina mentioned to Gilinsky that Defendant had been recording his telephone calls, and discussed the emails from Elijah Pearson. Spina Aff. P24. Gilinsky was already aware that the FBI had recovered emails from Defendant indicating that Defendant had reacquired images of the two victims in the spring of 2004, and that indicated that Defendant might attempt to manipulate the videos. Gilinsky Aff. P11. AUSA Spina does not recall disclosing the existence or contents of any of Defendant's notes or the "Case18Clips" during this meeting. Spina Aff. P24. Gilinsky confirmed that he had provided sexually explicit images of the minor victim to Defendant after the originals had been seized by law enforcement. Spina Aff. P23; Gilinsky Aff. P12. Gilinsky also advised that Defendant had expressed an intention, *inter alia,* to manipulate the audio portions of these video tapes to make it appear that the minor victims stated that they were 18 years of age or older. Gilinsky Aff. P12. After the meeting, Gilinsky entered into a formal cooperation agreement and testified before the grand jury. Id. P13. Gilinsky asserts that he has never been asked or pressured by the [*20] Government to lie, and instead was advised repeatedly to "simply tell the truth." Id.

On January 11, 2006, a 74 count Second Superceding Indictment was returned. In addition to charging the same counts as the Superceding Indictment, it charged three new counts pertaining to Defendant's conduct in April 2004. See Second Sup. Indict. Counts 69 & 70 (charging separate violations of *18 U.S.C. §§ 2252A(a)(2) & 2256(8)*); and Count 73 (charging a violation of *18 U.S.C. §§ 2252A(a)(5)(B) & 2256(8)*). The government contends that all of the items seized on December 1, 2005, except the 2.23 GB encrypted folder contained on the Western Digital hard drive, have been returned to Defendant and that no information contained on the items seized was deleted or modified in any way. See Fallon Aff. P30.

On February 17, 2006, Defendant filed the instant Second Omnibus Motion. With that motion Defendant submitted an affidavit in which he attests that:

> (2) My father, Elijah Pearson, . . . is one of the retained attorneys working on my case.
>
> (3) Much of the material seized contained confidential [*21] attorney client files and communications kept on the seized computers.

> (4) Much of the material seized constituted attorney work product, both by Elijah Pearson and by Kindlon and Shanks. [3] Key USA witness David Gilinsky has confirmed to me that the USA has used said attorney work product, conveyed in his discussion with prosecutor Spina. Mr. Gilinsky also told me that the government has pressured him to lie.
>
> (5) Some of the material seized was exculpatory evidence, the loss of which severely prejudices me.
>
> (6) The legal documents seized represent a large part of my trial strategy, and their loss severely prejudices me, both because said material is now in the hands of the government, and because I no longer have access to much of said material. Relevant files seized include about twenty interviews with several important witnesses and a statement by key USA witness, Mr. Gilinsky, on witnessing evidence altering by the FBI (none of which has been seen yet by Kindlon and Shanks).
>
> (7) Audio analysis and processing software for my defense was seized.
>
> (8) All copies of finished media work product intended for trial, prepared with my attorney, Elijah Pearson, have [*22] been seized on December 1, 2005. ...

Pearson Aff. [dkt. # 50]. Gilinsky denies that he told Pearson that the Government had used "attorney work product," and avers that he has not spoken to Defendant or Defendant's father since December 5, 2005 (the day Gilinsky retained counsel). Gilinsky Aff. P15.

> 3 Defendant's counsel-of-record, Terence L. Kindlon, Esq., submits an affidavit that appears to contradict this assertion. Kindlon asserts:
>
> > 19. Much of the material seized contained confidential attorney client communications and work product kept on the seized computers. According to Abraham Pearson the material included extensive notes by Elijah and Abraham Pearson on the planned cross examination of approximately twenty witnesses, including David Gilinsky. None of that particular material has been seen by the Office of Kindlon and Shanks, PC., and now it is in the possession of the government and the defense has no access to said material.
>
> Kindlon Aff. P19 (emphasis added).

The Government's [*23] opposition to the Second Omnibus Motion was sealed by order of the Hon. Norman A. Mordue, the District Judge originally assigned to this matter. On March 6, 2006, Judge Mordue recused himself from presiding over this case, and the case was re-assigned to the undersigned. See Order of Recusal [dkt. # 62]. On March 17, 2006, the Court received a letter from the Government which states as follows:

> Dear Judge McAvoy:
>
> I am writing to advise you that the prosecution of this matter has

> been reassigned to Jill Trumbull-Harris and Steve Grocki of the Department of Justice's Child Exploitation and Obscenity Section. In addition, the FBI has reassigned the investigation to a special agent who was recently transferred to the Bureau's Syracuse office from Baltimore. Special Agent Fallon and I will therefore not represent the government in this matter at trial. Rather, we will become, in effect, part of a "taint" team to ensure that the new attorneys and agent assigned are not exposed to any potentially privileged material. As a result, I will continue to represent the government on the current motions pending before the Court since they involve the allegedly privileged material.
>
> Although [*24] reassignment of this matter is not required under the law inasmuch as there was no intentional review of privileged material and no inappropriate use of any such material, the government has taken these steps in an abundance of caution to eliminate any possible claim of prejudice to the defendant as the case moves forward.

Spina 3/17/06 Letter [dkt. # 67].

III. DISCUSSION

A. Dismissal of Indictment based upon Violation of the Defendant's Attorney-Client Privilege

Defendant moves to dismiss the Second Superceding Indictment on the grounds that his *Sixth* and *Fifth Amendment* Rights were violated in obtaining this Indictment. He alleges that the Government improperly had access to, and used, materials protected by the attorney-client privilege and attorney work product in obtaining the Second Superceding Indictment. More specifically, he alleges that privileged information contained in computer media seized pursuant to the search warrant executed on December 1, 2005 was used to obtain the cooperation of a witness (Gilinsky) who testified before the grand jury on December 14, 2005. He further asserts that the computers and computer media contained exculpatory [*25] evidence which is now lost. In the alternative, Defendant seeks the dismissal of Counts 69, 70 & 73, which were added after the December 1, 2005 seizure.

On this motion, the Court will presume that Defendant's father is part of Defendant's defense team. Further, the Court will presume that, at the very least, Defendant's type-written notes constitute privileged material. See *United States v. Defonte, 441 F.3d 92, , 2006 WL 623603, at *3 (2d Cir. March 14, 2006)*(holding that defendants handwritten notes of what he wanted to discuss with his attorney - and which he subsequently discussed with counsel - fit squarely within the scope of the attorney client privilege).

1. *Sixth Amendment*

In determining whether there has been an intrusion into the attorney-client relationship in violation of a defendant's *Sixth Amendment* rights, Courts have examined the following factors: (1) whether there was an intentional intrusion into the attorney-client relationship to gather confidential privileged information, or whether the intrusion was inadvertent; (2) whether evidence to be used at trial was obtained directly or indirectly by the government intrusion; [*26] (3) whether the prosecution obtained details of the defendant's trial preparation or defense strategy; and (4) whether the government, directly or indirectly, used or will use evidence obtained as a result of the intrusion to the substantial detriment of the defendant. *Weatherford v. Bursey, 429 U.S. 545, 97*

S.Ct. 837, 51 L.Ed.2d 30 (1976). The Second Circuit has held that "unless the conduct of the Government has ... been ... manifestly and avowedly corrupt, a defendant must show prejudice to his case resulting from the intentional invasion of the attorney-client privilege." *United States v. Schwimmer, 924 F.2d 443, 447 (2d Cir.)*, cert. denied *502 U.S. 810, 112 S. Ct. 55, 116 L. Ed. 2d 31 (1991)*(citations omitted); *United States v. Gartner, 518 F.2d 633, 637 (2d Cir.)*("Where, however, the conduct of the Government has not been so manifestly and avowedly corrupt, the courts have applied a different and less rigid rule which attempts to measure the harm or prejudice, if any, to the defendant rather than punish the prosecutor by freeing the defendant."), cert. denied, *423 U.S. 915, 96 S. Ct. 222, 46 L. Ed. 2d 144 (1975)*. Here, defendant cannot show manifest corruption, [*27] intentional invasion or actual prejudice

There is no evidence of manifest corruption by the Government in searching Defendant's residence and seizing the computers and computer media to which he had access. The search warrant was sought, and executed, based upon a demonstrated belief that there existed evidence of Defendant's continued violation of the child pornography laws at his residence and on the computers to which he had access. The uncontested facts indicate that at the time the Government executed the search warrant the Government had a legitimate reason for obtaining and executing the search warrant - namely, that Defendant had committed further crimes and a well founded belief that the evidence of those crimes might be contained on the computers and computer media in his residence. This belief was founded upon evidence that the Government legitimately obtained from David Gilinsky's computer.

Further, there exists little if any evidence of intentional intrusion into the attorney-client relationship at the time the computers and computer media was seized and the FBI began its forensic evaluation of these materials. At the time the search warrant was issued and executed, [*28] there existed no evidence that Defendant's father was participating in his defense. Indeed, the father's letter to the United States Attorney claimed the opposite. There is no competent evidence before the Court that Defendant or his father made any representation to this effect before Defendant's handwritten notes were discovered and read by the FBI case agent. The FBI searched the computers and computer media by using search terms such as the victim's names or nicknames, and Gilinsky's name, or by looking for picture, video, or audio files that might be evidence of Defendant's further commission of child pornography-related crimes and otherwise avoided text material that might be privileged.

There is an indication, however, that shortly after the seizures, Defendant's father put the Government on notice that he was participating in his son's defense. Presuming that Elijah Pearson's December 2, 2005 letter reached the United States Attorney's Office the same day that it reached Judge Mordue's Chambers (December 6, 2005), the Government was on notice from that day forward that privileged material might be contained on the seized computer material. Even accepting this proposition, [*29] however, the Government's actions since December 6, 2005 have served to ameliorate any prejudice that might otherwise have befallen Defendant. AUSA Spina acted appropriately in sealing Defendant's notes upon reviewing them, see *United States v. Weissman, 1996 U.S. Dist. LEXIS 19067, 1996 WL 751386 * 12 (S.D.N.Y. 1996)*(Intrusion not intentional where AUSA had no idea what the file contained until information had fallen into his hands and he read the privileged memorandum), and creating a "taint team" to prevent the prosecution from gaining any advantage from the review of any potentially privileged material.

In addition, the Government indicates that it does not intend to offer any evidence from the December 1, 2005 seizure other than any sexually explicit images of the minors possibly contained in encrypted files and the videos contained in the "Case18Clips" folder. Sexually explicit images of minors (if they exist) and videos of women stating their ages do not constitute attorney-client material and, therefore, are not protected even assuming they were found in files marked "privileged," "confidential," or "attorney work product." See *United States v. Pelullo, 917 F. Supp. 1065, 1077(D.N.J. 1995)* [*30] ("While Pelullo may not have waived a privilege claim, the manner in which he packaged and warehoused his vast array of documents created conditions which negate his charge that the government deliberately seized documents which it knew to be privileged."). Given the information tending to indicate that Defendant was contemplating manipulating the re-acquired videos of the minor victims, the "Case18Clips" folder is exempted from the protection of the attorney-client privilege under the crime-fraud exception. See *John Doe, Inc. v. United States (In re John Doe, Inc.), 13 F.3d 633, 636 (2d Cir. 1994)*.

Further, even assuming, arguendo, that there was an intentional violation of Defendant's *Sixth Amendment* rights, there is no per se rule requiring dismissal of the indictment. "[A]bsent demonstrable prejudice, or substantial threat thereof, dismissal of the indictment is plainly inappropriate, even though the violation may have been deliberate." *United States v. Morrison, 449 U.S. 361, 364-65, 101 S. Ct. 665, 66 L. Ed. 2d 564 (1981)*. In order to establish demonstrable prejudice, or the substantial threat thereof, it must be shown at the very least that the confidential information was used for the benefit of the government [*31] or the detriment of the defendant. See *Bishop v. Rose, 701 F.2d 1150, 1156-57 (6th Cir. 1983)*(actual use of notes by prosecutor drafted by defendant to his attorney, at his attorney's request, to cross-examine the defendant at trial constituted demonstrable prejudice). Mere exposure of the government to privileged materials is insufficient to warrant relief. See *Schwimmer, 924 F.2d at 443* ("[M]ere 'tangential [] influence ... [that privileged information may have on] the prosecutor's thought processes in ... preparing for trial' [is] not an unconstitutional use."); cf. *United States v. Rivieccio, 919 F.2d 812, 815 (2d Cir. 1990)*(To the extent government's thought processes or questioning of witnesses were influenced by defendant's immunized grand jury testimony, any such use was merely tangential and was not a prohibited use in the defendant's prosecution); *United States v. Noriega, 764 F. Supp. 1480, 1489 (S.D.Fl. 1991)*("Yet the simple fact of communication [of the privileged information to the prosecution] is insignificant for *Sixth Amendment* purposes if there is no gain to the prosecution or adverse [*32] impact on the defendant as a result.").

The Second Circuit has noted that prejudice can be shown by establishing "that a prosecution witness testified concerning privileged communications, that prosecution evidence originated in such communication, or that such communications have been used in any other way to the detriment of the defendant." *United States v. Ginsberg, 758 F.2d 823, 833 (2d Cir. 1985)*. Yet, despite Defendant's conclusory allegations to the contrary, there is no evidence that the Government used Defendant's notes, or any other arguably privileged material seized on December 1, 2005, to convince Gilinsky to testify before the Grand Jury the second time. The recorded telephone calls with Gilinsky, and the emails from Elijah Pearson to Gilinsky, were not confidential because they were communications with a third party. Further, the telephone calls were not contained in a file marked confidential, and were properly examined in the first instance to determine whether they were illegal video files. Once identified as telephone conversations with Gilinsky, it was permissible to listen to them to determine whether they contained evidence of the pur-

ported April [*33] 2004 exchange of child pornography.

Moreover, even had Gilinsky been told about privileged information, such indirect use is not prohibited. See *Schwimmer, 924 F.2d at 446*. At the time the government interviewed Gilinsky, it had recovered incriminating emails from his computer which indicated that he had provided Defendant with sexually explicit images of the minors after he was charged. Gilinsky had already been cooperating in the Government's investigation and had previously been interviewed and testified before a federal grand jury. Gilinsky's decision to testify on December 14, 2005 appears to be based upon the fact that the Government recovered evidence from *his* computer indicating that he provided Defendant with child pornography in April 2004, and that Gilinsky wanted to enter a cooperation agreement to protect himself. Still further, a review of the grand jury minutes reveals no indication that the Government relied on any arguably privileged material in its presentation to the Grand Jury, and there is no basis to conclude that the Government pressured Gilinsky to lie before the Grand Jury.

To the extent Defendant argues that the fact that the Government [*34] has read his alleged trial preparation notes constitutes impermissible "use", this claim is rejected. As indicated above, these notes have been sealed and the Government has created a taint team to prevent any impact upon the prosecution form these notes. Given the steps taken by the Government to protect the defendant from any prejudice arising from the review of protected material, Defendant's motion to dismiss the Second Superceding Indictment, or any part thereof, on the grounds of a *Sixth Amendment* violation, is denied. See *United States v. Singer, 785 F.2d 228, 234-35* (since district court's remedial measures were adequate, dismissal of Indictment was not required even where the government violated a defendant's *sixth amendment* rights by intentionally procuring and reviewing an attorney-client file and it was determined that such conduct threatened to create prejudice at a retrial).

2. *Fifth Amendment*

Defendant's assertion that the computers and computer media contained exculpatory evidence and material to prepare his defense that is "now lost" appears to form the basis of his *Fifth Amendment* challenge to the Second Superceding Indictment. In order to obtain the drastic [*35] remedy of dismissing an indictment or reversing a conviction based upon a claim of governmental conduct in violation of the *Fifth Amendment*, "a defendant must establish that the government engaged in outrageous behavior in connection with the alleged criminal events and that due process considerations bar the government from prosecuting...." *United States v. Cuervelo, 949 F.2d 559, 565 (2d Cir. 1991)*; see also *United States v. Russell, 411 U.S. 423, 431-32, 93 S.Ct. 1637, 1642-43, 36 L.Ed.2d 366 (1973)*. The conduct must be so egregious that it simply shocks the conscience. See *United States v. Rahman, 189 F.3d 88, 131 (2d Cir. 1999)*, cert. denied, *528 U.S. 1094, 120 S. Ct. 830, 145 L. Ed. 2d 698 (2000)*. Dismissal of an indictment based upon such conduct is rare. *United States v. Myers, 692 F.2d 823, 847 (2d Cir. 1982)*, cert. denied, *461 U.S. 961, 103 S. Ct. 2437, 103 S. Ct. 2438 (1983)*; *United States v. Artuso, 618 F.2d 192, 196 (2d Cir. 1980)*. It has been noted that the power to dismiss a case on this basis should be used sparingly. *United States v. Santana, 6 F.3d 1, 10 (1st Cir. 1993)*. "[T]he burden of establishing [*36] outrageous investigatory conduct is very heavy." *Rahman, 189 F.3d at 131*. "Such a claim rarely succeeds." *United States v. LaPorta, 46 F.3d 152, 160 (2d Cir. 1994)*.

Defendant has not provided any particulars of the material that is now purportedly "lost," and the Government has asserted that it returned, unaltered, all of the seized material other than the encrypted files. Thus, it may be that the encrypted files contain some type of "ex-

culpatory evidence" or trial preparation material that Defendant now believes is lost. The Court finds that the best way to resolve this matter is to have the Defendant, his attorneys, and the Government's "taint team" present during an *in camera* hearing at which time the Defendant will provide a more definite statement as to the particular location of the material he claims is lost, and the purported location of the material before the December 1, 2005 search. If the material is contained on the encrypted files and if the password is not otherwise required to be produced (see discussion below regarding Defendant's *Fifth Amendment* challenge to the trial subpoena, infra), Defendant can choose to voluntarily [*37] provide the password for the file or files he contends contains exculpatory material and/or trial preparation material. The files will be reviewed in the presence of the participants to this hearing. If the material is exculpatory, it will be provided to Defendant and the taint team will be ordered not to divulge the information to the Government's trial team. Under such circumstances, the Court will determine what remedy, if any, Defendant is entitled to. If Defendant asserts that there exists some other exculpatory evidence or trial preparation material other than which might be contained on the encrypted files, then he should be prepared to present evidence of this material at this hearing. The Government's "taint team" will then respond to the arguments and/or factual assertions, and the Court will rule accordingly. The "taint team" will be ordered not to divulge to the trial team the nature of the alleged "lost" material.

Therefore, the Court reserves on Defendant's *Fifth Amendment* challenge seeking dismissal of the Second Superseding Indictment. The hearing will be held immediately prior to trial.

B. Dismissal of Counts 67-73 as Multiplicitous

Defendant renews portions [*38] of his previous motion alleging that various counts of the indictment impermissibly charge him with the same offenses. As to the new counts contained in the Second Superceding Indictment, he argues that count 73, charging him with the possession of sexually explicit images of Jane Does # 1 & 2, should be dismissed since he is charged with receiving the same images in Counts 69 and 70.

For the reasons set forth in Judge Mordue's November 3, 2005 Decision on the same issue raised in the first Omnibus Motion, the motion is denied without prejudice to renewal at trial.

C. Title *18, United States Code, Section 2251(a)*, Which Criminalizes the Production of Child Pornography, Is a Valid Exercise of Congressional Authority under the *Commerce Clause*.

Defendant once again asserts that counts 1-66 of the Indictment should be dismissed because there are insufficient allegations that his activity substantially affected interstate commerce and, therefore, no federal jurisdiction exists. For the reasons set forth in Judge Mordue's November 3, 2005 Decision on the same issue raised in the first Omnibus Motion, the motion is denied.

D. Suppression of Physical Evidence [*39]

Defendant asks the Court to suppress all the physical evidence recovered from his residence pursuant to a search warrant on December 1, 2005 on the grounds that the evidence was seized in violation of Defendant's attorney-client privilege. In addition, Defendant asserts that since the affiant of the search warrant affidavit failed to inform the magistrate judge that the location to be searched was the law office of Defendant's father, all the evidence should be suppressed. In the alternative, the defendant seeks a Franks hearing on this issue.

In *Franks v. Delaware, 438 U.S. 154, 98 S.Ct. 2674, 57 L.E.2d 667 (1978)*, the Supreme Court ruled that in limited circumstances a de-

fendant may be entitled to an evidentiary hearing concerning inaccuracies in an affidavit in support of a search warrant. To be entitled to such a hearing, a defendant must offer proof that statements in the affidavit are false and that the affiant made the false statement knowingly or with reckless disregard for the truth. *United States v. Malsom, 779 F.2d 1228, 1235 (7th Cir. 1985)*; *United States v. Rodgers, 732 F.2d 625, 628 (8th Cir. 1984)*; [*40] *United States v. Marcello, 731 F.2d 1354, 1358 (9th Cir. 1984)*. The defendant must also establish that without the allegedly false statement, the magistrate would not have issued the warrant. *Franks 438 U.S. at 171-72*; *Malsom, 779 F.2d at 1235*. Unless a defendant offers substantial proof that the affiant's statement was deliberately false or demonstrated reckless disregard for the truth, the defendant is not entitled to an evidentiary hearing. *United States v. Phillips, 727 F.2d 392, 400 (5th Cir. 1984)* (conclusory allegations insufficient to merit hearing); *United States v. Reed, 726 F.2d 339, 341-42 (7th Cir. 1984)* (self-serving statements not substantial preliminary showing required to obtain Franks hearing). Allegations of negligence or innocent mistake do not warrant an evidentiary hearing. *United States v. Reed, 726 F.2d at 342*; *United States v. Ciammitti, 720 F.2d 927, 932 (6th Cir. 1983)*, cert. denied, *104 S. Ct. 2342, 466 U.S. 970, 80 L. Ed. 2d 816 (1984)*. If a defendant fails to meet this threshold burden of providing substantial proof, the defendant's motion for an [*41] evidentiary hearing on this issue must be denied. *United States v. Orozco-Prada, 732 F.2d 1076, 1089 (2d Cir.)*, cert. denied, *105 S. Ct. 154, 469 U.S. 845, 83 L. Ed. 2d 92 (1984)* (failure to present evidence supporting allegation that admittedly erroneous statements in affidavit were made intentionally or recklessly justified denial of Franks hearing).

Here, there exists no evidence that the Government agent made any false statements in his search warrant affidavit. As noted above, the Government was unaware that the defendant's father was one of his attorneys. In addition, Magistrate Judge Treece, who signed the search warrant, was apparently aware that the defendant's father was an attorney since he had presided over Defendant's detention hearing and was told this information during this hearing. See Spina Aff. P32. One of the conditions of Defendant's release was that he reside with his father. In addition, Defendant's father had apparently written the magistrate judge prior to the issuance of the warrant and indicated that he was an attorney. Id.

Further, for reasons discussed above, there is no basis to suppress evidence on the claimed violation of the attorney-client [*42] privilege. The evidence that the Government intends to offer in this case from the December 1, 2005 search and seizure is not governed by the attorney client privilege. [4] Therefore, the motion to suppress and for a Franks hearing is denied.

4 In its Memorandum of Law in Opposition to Defendant's Second Omnibus Motion, the Government contends:

> At this time, the only evidence the government seeks to introduce from the items seized on December 1, 2005, are: (1) any sexually explicit images of minors involved (in the event they are located on the encrypted computer media), as direct evidence of reacquiring and receiving the images; (2) evidence that various files on computer media, including a 2.3 gigabyte file on an external hard drive, are encrypted, as consciousness of guilt; and (3) the "Casel 8Clips", as consciousness of guilt.

Govt. Mem. L. p. 20.

E. Request for the Return of Property

Defendant alleges that the Government improperly seized privileged attorney-client material [*43] on December 1, 2005, and asks that "any and all property seized" be returned.

Rule 41(g) of the Federal Rules of Criminal Procedure provides:

> A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return. The motion must be filed in the district where the property was seized. The court must receive evidence on any factual issue necessary to decide the motion. If it grants the motion, the court must return the property to the movant, but may impose reasonable conditions to protect access to the property and its use in later proceedings.

Fed R. Crim. P. 41(g).

A *Rule 41* motion may be denied "if the defendant is not entitled to lawful possession of he seized property, the property is contraband or subject to forfeiture or the government's need for the property as evidence continues." *United States v. Van Cauwenberghe, 934 F.2d 1048, 1061 (9th Cir. 1991)*. Retention of evidence by the government is proper if the property is needed in an investigation or prosecution. *Ramsden v. United States, 2 F.3d 322, 326 (9th Cir. 1993),* [*44] cert. denied, *511 U.S. 1058, 114 S. Ct. 1624, 128 L. Ed. 2d 349 (1994)*; *Sovereign News v. United States, 690 F.2d 569, 577 (6th Cir. 1982)*, cert. denied, *464 U.S. 814, 104 S. Ct. 69, 78 L. Ed. 2d 83 (1983)*. According to the Advisory Committee Notes to the 1989 Amendment of *Rule 41(e)*, "reasonableness under all the circumstances must be the test when a person seeks the return of property." "However, 'if the United States' legitimate interests can be satisfied even if the property is returned, continued retention of the property would become unreasonable.'" *Ramsden. 2 F.3d at 326* (quoting Advisory Committee's Note to *Rule 41*). The burden is on the moving party to show that the seizure was illegal and that he is entitled to lawful possession of the property. *Cauwenberghe, 934 F.2d at 1061.*

The Court finds that under the circumstances, the search warrant was properly issued and the computers and computer media from Defendant's residence were properly seized and searched. As indicated above, other than the Western Digital hard drive containing the 2.23 gigabyte encrypted folder, all of the items seized pursuant to the warrant have been returned to the defendant. See Fallon Aff. P30. [*45] However, copies of various items have been retained. Id. Some of these items have been retained because they contain encrypted media which may contain sexually explicit images of the minor victims. Id. The remainder have been retained purportedly to protect the Government from claims by Defendant that evidence has been lost or destroyed. Id. The Government contends that, other than attempts to decrypt information to search for image files, no further searches of these items will occur.

Given the Government's representation, the fact that a taint team has been established by the Government, and that a pre-trial hearing will be held to determine the contents of the encrypted files, the motion is denied with leave to renew following the pre-trial hearing.

F. Requests for Discovery

Defendant has made a number of discovery requests which the Court will address seriatim.

Request (a) "All materials seized on December 1, 2005." The Government contends that the following material was seized on December 1, 2005: (1) a 400 GB Sony Vaio Computer, Model PCV 1152, S/N 3000001; (2) a Sony Vaio Computer, model PCV-RX550,

s/n A8023273A 0204338; (3) a Western Digital external [*46] hard drive, s/n WCAEK1534T54; (4) a SONY thumb drive; (5) Lexor thumb drive; and (6) over one hundred computer disks. The Government further contends that other than the Western Digital hard drive, it has provided Defendant with all these items. In addition, except for the 2.3 gigabyte encrypted folder, the Government has provided Defendant with a copy of this hard drive. For the reasons discussed above, this disclosure by the Government is sufficient at the present time. After the pre-trial hearing, the Court will determine what, if any, additional discovery must be made.

Request (b) "All transcripts and/or copies of recordings or any and all audio/video tape recordings...." The government asserts that transcripts of any audio/video tape recordings are currently being prepared by the Government. The Government further asserts that transcripts will be provided to the defense once complete and that audio portions of these tapes have previously been provided to Defendant. The Government further contends that the videos seized from Defendant's residences were made available to Defendant and he, in fact, viewed a number of them during a discovery conference. The Government represents [*47] that it will make the videos available to Defendant and any expert retained by Defendant. This disclosure is sufficient. The Government need not provide copies of the visual portions of computer videos that purportedly depict the actual production of child pornography. See *United States v. Horn, 187 F.3d 781 (8th Cir. 1999)*; *United States v. Kimbrough, 69 F.3d 723, 731 (5th Cir. 1995)*(*Rule 16* does not provide that child pornography, which is illegal contraband, can be distributed to, or copied, by defense); *United States v. Husband, 246 F. Supp.2d 467 (E.D.Va. 2003)*.

Request (c) "any and all drafts of the transcripts, as well as all notes of the individuals preparing the transcripts." The Government asserts that, to the extent discoverable, any drafts of transcripts will be provided as Jenks Act material. This disclosure is sufficient.

Request (d) "all voice exemplars." The Government asserts that "at this time, there are no voice exemplars." Thus, there is no disclosure requirement for voice exemplars.

Request (e) "any and all records regarding the decision that this case be prosecuted federally." Defendant has provided no authority [*48] for this request. The Government argues that records regarding the decision that the case would be prosecuted federally, rather than in state court, are not discoverable. The Court agrees. This request appears to fall squarely within *Fed. R. Crim. P. 16(a)(2)* which exempts from disclosure "reports, memoranda, or other internal government documents made by an attorney for the government or other government agent in connection with investigating or prosecuting the case." See *United States v. Koskerides, 877 F.2d 1129, 1133 (2d Cir. 1989)*. Because the request specifically seeks materials concerning the decision to prosecute this matter, the request is denied.

Request (f) "a complete designation of which recordings or portions thereof will be used ... at trial." The government asserts that

> [a]ll recordings and images created by Defendant and seized from his home which depict the two minors engaged in sexually explicit conduct will be introduced at trial. These items are more specifically set forth in the indictment by volume number. In addition, videos and still images depicting commercial child pornography will be introduced [*49] at trial. All these recordings and images and the others referred to in the indictment are available for inspection and review by the defendant. By letter dated July 22, 2004, the govern-

> ment informed the defendant that all the images were available for his review. Thereafter, the defendant viewed a number of these videos during a discovery conference.

Govt. Mem. L. p. 30. This representation is sufficient.

Request (g) "all court documents and transcripts related thereto." It is not clear to the Court or the Government what Defendant is seeking in this request. See id. The Government represents that the New York State search warrants, applications and affidavits have already been provided to the defense, and documents and transcripts from this Court are available from the Court Clerk's Office. The motion in this regard is denied.

Request (h) "all police reports." Brady impeachment material (see *Brady v. Maryland, 373 U.S. 83, 87, 83 S. Ct. 1194, 10 L. Ed. 2d 215 (1963))*, as well as Giglio material (see *Giglio v. United States, 405 U.S. 150, 154, 92 S. Ct. 763, 31 L. Ed. 2d 104 (1972))*, must be supplied to Defendant with the statements of witnesses producible under *18 U.S.C. § 3500(a)* [*50] and *(b)* of the Jencks Act, which is to say these need not be produced until after the relevant witness has testified on behalf of the government. See *United States v. McKinzie, 1996 U.S. App. LEXIS 27147, 1996 WL 590730, at * 3 (N.D.N.Y. Oct. 03, 1996)*(citing *United States v. Higgs, 713 F.2d 39, 44 (3d Cir. 1983))*. It is the normal practice in the Northern District to require Jencks Act material to be handed over after the jury is selected for trial. To the extent that such material has not been handed over to date, the Court can find no reason to depart from its usual practice and order early production.

G. Identification/Preclusion of "Bad Act" Evidence

Defendant has requested that the Court direct the Government to furnish evidence of all prior bad acts or similar acts of defendant which it will seek to have admitted at trial pursuant to *Rule 404(b) of Federal Rules of Evidence.* In addition, the defendant specifically seeks to exclude any prior bad acts.

In its prior motion response the Government identified prior bad acts it intends to introduce at trial. In addition, in subsequent correspondence, the Government identified additional [*51] "bad acts" evidence it intends to use. For the reasons stated in Judge Mordue's November 3, 2005 Decision, Defendant's motion is denied. Questions of admissibility of particular evidence will be addressed immediately prior to trial.

H. Request for Leave to File Additional Motions

Defendant will be permitted to make additional motions only for good cause shown. The Court will not, however, accept additional motions that rehash the issues presented in the current omnibus motion and will not grant leave to make additional motions based on information and legal arguments which could have been brought through the exercise of due diligence as part of the instant motion. The Court will exercise its discretion in determining the validity of any future motions. Accordingly, that part of the Omnibus Motion seeking leave to submit additional motion is **GRANTED** as set forth herein.

I. Motion to Quash Trial Subpoena

Defendant also moves to quash a subpoena issued in early 2006 which compels him to produce for the Government:

> Any and all passwords, keys, and/or log-ins used to encrypt any and all files, including but not limited to, Steganos encrypted files, [*52] contained on the following

items recovered from your residence pursuant to a search warrant on December 1, 2005, and currently in the government's possession:

> 1. A Western Digital hard drive, s/n WCAK 1534754;
>
> 2. A copy of a SONY Microvault USB flash drive;
>
> 3. A copy of a SONY Microvault USB flash drive;
>
> 4. A SONY vaio desktop computer, model PCU 1152, s/n/ A222663W;
>
> 5. A SONY DVD-R computer disk, labeled "Archive and BU 8/04."

Trial Subpoena, Govt. Ex. 1.

Defendant bases his motion to quash on two grounds. One, he asserts that his *Fifth Amendment* right not to be compelled to testify against himself protects him from having to produce the passwords. Two, he asserts that the files contain attorney-client privileged information to which the Government should not have access. For the reasons that follow, the Court will hold a factual hearing on this motion. [5]

> 5 In a letter to the Court dated May 22, 2006, Defense Counsel asserts that the "trial subpoena issue [is] moot" because a recent newspaper article reported that "a law enforcement official close to the case said the FBI already has accessed the files but the agency is reluctant to testify about the methods it uses to crack encrypted files" due to national security concerns. Sprotbery 5/22/06 ltr & Ex. 1 [dkt. # 80]. The Court does not find that the pending motion is moot. While the information in the newspaper, if correct, might obviate the need for the subpoena (AUSA Spina has filed a letter indicating that the information in the newspaper is not accurate), the subpoena was issued by the Government. Until the Government withdraws the subpoena, it is still in effect. The motion to quash the subpoena was brought by Defendant, and the Court does not read Defendant's letter as an application to withdraw the motion or a concession that the motion to quash is moot because he has complied with the subpoena. If defense counsel is asserting that, under the circumstances, the refusal of the Government to withdraw the subpoena is an abuse of the subpoena power, then he should so state and be prepared to address the issue (with both factual and legal support) at the pre-trial hearing.

[*53] The *Fifth Amendment* privilege against self-incrimination "protects a person ... against being incriminated by his own compelled testimonial communications." *Fisher v. United States, 425 U.S. 391, 409, 96 S. Ct. 1569, 48 L. Ed. 2d 39 (1976)*; see *U.S. Const., Amend. V* ("No person? shall be compelled in any criminal case to be a witness against himself."). For a communication to be protected by the *Fifth Amendment*, it must be compelled, testimonial, and incriminating in nature. *Fisher, 425 U.S. at 408*. Failure to satisfy any of these three elements defeats the application of the *Fifth Amendment* privilege.

It is well-settled that "if the party asserting the *Fifth Amendment* privilege has voluntarily compiled [a] document, no compulsion is present and the contents of the document are not privileged." *United States v. Doe, 465 U.S. 605,*

612 n. 10, 104 S. Ct. 1237, 79 L. Ed. 2d 552 (1984)(Doe I); *Fisher, 425 U.S. at 409-410* (Voluntarily produced documents are not compelled and, therefore, do not enjoy *Fifth Amendment* protection.). The Government argues that given the length and unrelated characters of the password, see Def. March 11, 2004 e-mail to Gilinsky ("The thing encrypts [*54] immediately (live/realtime) and will have a password like: eolKleGH93*vfOY3Gw4kn&jd ."), Defendant more than likely reduced the password to writing. Production of this voluntarily created writing would not, the Government argues, constitute compulsion. Defendant has not responded to this argument.

The Government also argues that the password itself is not incriminating, and therefore, Defendant has no *Fifth Amendment* privilege from producing it. Again, Defendant has not responded to the argument. Instead, Defendant argues that "[w]hile the *content* of the seized materials may not be protected by the *Fifth Amendment* because the production of said materials was not compelled or testimonial," the "act of producing the decryption information ... would violate the *Fifth Amendment* because it would 'communicate testimonial aspects as to the existence of the documents, possession or control of the documents, or the authenticity of the documents."" Def. Mem. L. in Supp. Mot. to Quash, pp. 1-2 (quoting *In re Grand Jury Proceedings, 41 F.3d 377, 379 (8th Cir. 1994))*(emphasis in original). This argument invokes the *Fifth Amendment* "act of production" doctrine. [6]

> 6 By proceeding directly to the "act of production" argument, Defendant essentially concedes that the password itself carries no *Fifth Amendment* privilege. See *In re Hyde, 235 B.R. 539, 542-43 (S.D.N.Y. 1999)*("Our Court of Appeals has stated that the *Fifth Amendment* does not protect the contents of voluntarily prepared documents, either business or personal. Hyde has made no claim that the documents were not voluntarily prepared. The Bankruptcy Court, therefore, correctly determined that the contents of the books and records at issue are not privileged. Even if the contents of documents are not privileged, however, the act of producing those documents might be.")(citing *In re Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992, 1 F.3d 87, 93 (2d Cir. 1993).*

[*55] The act of production doctrine was developed by the Supreme Court in a series of cases that addressed whether the act of producing otherwise unprivileged documents was protected under the *Fifth Amendment's self-incrimination clause* . See *Fisher, 425 U.S. at 409*; *Doe I, 465 U.S. at 612*; *Doe v. United States, 487 U.S. 201, 209, 108 S. Ct. 2341, 101 L. Ed. 2d 184 (1988)*("Doe II"); *Baltimore City Dept. of Social Services v. Bouknight, 493 U.S. 549, 110 S. Ct. 900, 107 L. Ed. 2d 992 (1990).* The focus in such cases is on whether the act of producing the document (or some other thing sought) has "testimonial aspects" such as confirming the existence of an otherwise unknown incriminating document, establishing that the producer of the document had ownership or control of the document, or authenticating the document by establishing that the producer of the document believed that the document was what the subpoena requested. *Doe I, 465 U.S. at 613*; see also *United States v. Hubbell, 530 U.S. 27, 36-37, 120 S. Ct. 2037, 147 L. Ed. 2d 24 (2000)*(The "act of production" doctrine has been recognized as protecting individuals from incriminating themselves by being compelled to produce documents where [*56] the production could implicitly communicate incriminating facts, such as the admission that "papers existed, were in [the producing party's] possession or control, and were authentic."); *In re Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992, 1 F.3d 87, 93 (2d Cir. 1993)*, cert. denied sub nom. *Doe v. United States, 510 U.S. 109, 114 S. Ct. 920, 127 L.Ed. 2d 214 (1994)*;

United States v. Walker, 982 F. Supp. 288, 290-91 (S.D.N.Y. 1999)(The act of production doctrine applies to production of documents that are not themselves privileged under the *5th Amendment* but which may have some testimonial impact and an incriminating effect if produced.)(citing *Doe I, 465 U.S. at 612*).

However, where the existence, ownership, control, or authenticity of the document (or thing) is a "forgone gone" conclusion, the testimonial aspect of production is minimized if not eliminated. See *Fisher, 425 U.S. at 411*. As the Supreme Court noted in Fisher, production of already-known documents that "add little or nothing to the sum total of the Government's information by conceding that he does have the papers" does not serve as a testimonial act deserving [*57] of *Fifth Amendment* protection. *Fisher, 425 U.S. at 411*; compare *Hubbell, 530 U.S. at 44-45* (holding that where the Government had not demonstrated prior knowledge of the existence or location of 13,120 pages of documents produced, and where the subpoena made broad, general requests, the act of turning over those documents qualified as compelled, testimonial self-incrimination falling under the protection of the *Fifth Amendment*).

In the Second Circuit, "the act of producing [otherwise unprivileged documents] in response to a subpoena may require incriminating testimony in two situations: (1) if the existence and location of the subpoenaed papers are unknown to the government; or (2) where production would implicitly authenticate the documents." *In re Grand Jury Subpoena Duces Tecum Dated October 29, 1992, 1 F.3d at 93* (citations and quotation marks omitted). Thus, "[t]he first prong in our Circuit's test for the act of production privilege asks whether the existence and location of the subpoenaed documents is known to the Government." *In re Hyde, 235 B.R. at 545* (citing *In re Grand Jury Subpoena Duces Tecum Dated October 29, 1992,1 F.3d at 93*. [*58] In this regard, the Second Circuit stated:

> Production may not be refused if the government can demonstrate with reasonable particularity that it knows of the existence and location of subpoenaed documents. Since Doe produced a copy of the calendar to the SEC and testified about his possession and use of it, its existence and location are "foregone conclusions," and his production of the original "adds little or nothing to the sum total of the Government's information."

In re Grand Jury Subpoena Duces Tecum Dated October 29, 1992, 1 F.3d at 93(quoting *Fisher, 425 U.S. at 411*)(other citations omitted).

In the instant case, compliance with the subpoena does not tacitly concede the existence or location of the computer files because the files are already in the Government's possession. Their existence is a foregone conclusion. Further, the Government has already concluded upon forensic examination that they are encrypted. The Government has also rightfully obtained information from Defendant indicating that he intended to encrypt certain files, and that Defendant was provided with encryption software. Thus, the existence and use of encryption [*59] software on the files recovered from Defendant is all but a forgone conclusion, and knowledge of the actual password adds little to what the Government already knows in this regard. The Government's knowledge is sufficient to meet its burden to overcome the first prong of the act of production privilege. See *Walker, 982 F. Supp. at 291-92* (and cases cited therein).

Under the second prong of this Circuit's test, the Court "must next determine whether production would 'implicitly authenticate' the documents." *In re Hyde, 235 B.R. at 545*. "Im-

plicit authentication occurs when an individual who receives a [subpoena] demanding production of documents complies with the [subpoena] and thereby implicitly testifies that he owns or at least possesses the documents." *Walker, 982 F. Supp. at 292* (quoting *United States v. Fox, 721 F.2d 32, 38 (2d Cir. 1983)*.

> Even when production could constitute authentication, however (i.e., when "a government official will one day be able to testify that he knows the documents in question belong to petitioner because petitioner produced them when asked," [*In re Subpoena Duces Tecum, 616 F. Supp. 1159, 1161 (E.D.N.Y. 1985)]),* [*60] production can be compelled "when the government can authenticate the documents without relying on any act by petitioner." Id.; see also [In *Re Grand Jury Subpoena Duces Tecum, 1 F.3d 87, 93 (2d Cir.1993)]* (authentication by other means negates claim of privilege).

Id.; see also *In re Hyde, 235 B.R. 546* ("While invocation of the act of production privilege does not automatically mean that it applies, in those cases that did not hold production privileged, there were means of authenticating the documents other than directly through the production sought.").

Here, on first blush, it would seem that compliance with the subpoena would not demonstrate an element of ownership or control of the files beyond what the Government already knows. Indeed, Defendant has already voluntarily asserted under oath that the seized files contain *his* material. See Pearson Aff. PP3-8 [dkt. # 50]. Yet, he has asserted in this same affidavit that some of the materials on the computers were prepared by his attorneys. See e.g. id. P8 ("All copies of finished media work product intended for trial, prepared with my attorney, Elijah Pearson, have been seized [*61] on December 1, 2005."). It is unclear whether Defendant asserts that any of the encrypted files were prepared by his attorneys, and, thus, whether production of the password could serve to implicitly authenticate all the encrypted files. Of course, to the extent that Defendant asserts that the encrypted files were prepared by his attorneys, Defendant would have no *Fifth Amendment* "act of production" argument against their disclosure (although he may have other grounds to prevent the disclosure of the information to the Government, discussed below). See *Fisher, 425 U.S. at 409-410.* [7]

7 In this regard the Court wrote in Fisher:

> [T]he *Fifth Amendment* would not be violated by the fact alone that the papers on their face might incriminate the taxpayer, for the privilege protects a person only against being incriminated by his own compelled testimonial communications. *Schmerber v. California [384 U.S. 757, 86 S.Ct. 1826, 16 L.Ed.2d 908 (1966)]*; *United States v. Wade, [388 U.S. 218, 87 S.Ct. 1926, 18 L.Ed.2d 1149 (1967)]*; and *Gilbert v. California [388 U.S. 263, 87 S.Ct. 1951, 18 L.Ed.2d 1178 (1967)]*. The accountant's workpapers are not the taxpayer's. They were not prepared by the taxpayer, and they contain no testimonial declarations by him. Furthermore, as far as this record demonstrates, the prepa-

> ration of all of the papers sought in these cases was wholly voluntary, and they cannot be said to contain compelled testimonial evidence, either of the taxpayers or of anyone else. The taxpayer cannot avoid compliance with the subpoena merely by asserting that the item of evidence which he is required to produce contains incriminating writing, whether his own or that of someone else.

Fisher, 425 U.S. at 409-410.

[*62] If Defendant asserts that some of the encrypted files were prepared by his father, production of the password would not serve to authenticate *all* the files protected by the password. However, production of the password would provide powerful evidence on the issue of authentication of the encrypted files that his father did not produce because it would provide a link in the chain of ownership and control of any incriminating encrypted files. See *Hoffman v. United States, 341 U.S. 479, 486, 71 S. Ct. 814, 95 L. Ed. 1118 (1951)*("The privilege afforded by the *Fifth Amendment* not only extends to answers that would themselves support a conviction under a federal criminal statute but likewise embraces those which would furnish a link in the chain of evidence needed to prosecute the claimant for a federal crime."). Given this potential, the burden falls on the Government to demonstrate means to authenticate the files other than through the act of producing the password. Accordingly, the Court will hold a factual hearing to address whether the Government can authenticate the files by evidence *other* than the production of the password.

Turning to Defendant's second argument to quash the subpoena, [*63] the Court finds that the asserted attorney-client privilege is an insufficient basis for the requested relief. The bald claim that the files contain attorney-client privileged material is not a basis to refuse production of the encryption password. At the pre-trial hearing, only the Government's taint team will be present (along with Defendant and his trial team) so the Court can fashion an appropriate remedy if the files contain protected material. If Defendant desires to voluntarily produce a password for certain files, or if the Court rules that the password must be produced, the Court can then examine the files to determine whether any contain attorney-client privileged material. If they do, the Court will issue an appropriate order protecting Defendant's constitutional right to counsel and to a fair trial.

IV. CONCLUSION

For the reasons discussed above, Defendant's Second Omnibus Motion is **DENIED** in all respects ***except:***

(a) to the extent that Defendant seeks to dismiss the Second Superseding based upon prosecutorial misconduct arising to the level of a *Fifth Amendment* violation, on which the Court RESERVES decision and will hold a pretrial hearing [*64] at which the Government's "Taint Team," the Defendant, and his lawyers will be present; and

(b) to the extent that this Decision and Order grants Defendant leave to make additional motions, or renew previous motions upon good cause shown.

Further, the Court **RESERVES** on Defendant's motion to quash the Government's subpoena, and will hold a pretrial hearing on this motion.

IT IS SO ORDERED

DATED: May 24, 2006

Thomas J. McAvoy

Senior, U.S. District Judge