

Computers  
Removed from  
residence



2. All computer equipment and electronic storage media that currently belongs to, or has ever belonged to, Jeffrey Epstein, including but not limited to central processing units ("CPUs"), laptop computers, keyboards, printers, modems, routers, hard drives, flash drives, thumb drives, CD-Roms, DVDs, floppy diskettes, digital cameras, and memory cards.
3. All documents and information related to the nature of the relationship between [REDACTED] and/or [REDACTED] and Mr. Jeffrey Epstein, including, but not limited to, retainer agreements; employment agreements; billing statements (whether submitted directly to Mr. Epstein or to a third party for reimbursement); records of the dates when services were performed and the hours worked; telephone logs or records of dates of communications with Mr. Epstein (or with a third party on Mr. Epstein's behalf); appointment calendars/datebooks and the like (whether in hard copy or electronic form) for any period when work was performed on behalf of Mr. Epstein or when any communication was had with Mr. Epstein (or with a third party on Mr. Epstein's behalf); and records of fee arrangements and payments received for work performed on Mr. Epstein's behalf.

The bases for the requested relief are as follows:

A. the compelled production of these items, assuming they exist, would violate Mr. Epstein's rights under the Fifth Amendment to the United States Constitution;

B. such production of these items, assuming they exist, would further violate Mr. Epstein's Sixth Amendment right to effective assistance of counsel as well as his attorney-client and work-product privileges;

C. the subpoenas are unreasonable and oppressive and overbroad and unparticularized, in violation of the Fourth Amendment to the United States Constitution, the Due Process Clause of the Fifth Amendment, and Fed. R. Crim. Proc. 17(c); and

D. the subpoenas call for purely private papers in violation of the Fifth Amendment under *Boyd v. United States*, 116 U.S. 616 (1886).

As further reason therefore, Mr. Epstein refers the Court to the Memorandum of Law incorporated herein.

## MEMORANDUM OF LAW

In or about March 2005, the Palm Beach Police Department initiated a criminal investigation of Jeffrey Epstein to determine whether he committed any criminal acts in connection with allegations that he paid women to provide massages to him in his home. According to information obtained by the local police, one or more of the women so engaged was under the age of 18 at the relevant time. Affidavit of Roy Black, Esq., sworn to July 17, 2007, annexed ("Black Aff.") ¶3. Following a 16 month investigation, on July 17, 2006, Mr. Epstein was charged under Florida law with one count of soliciting a prostitute, a third degree felony. That charge is still pending. Black Aff. ¶5.

In the fall of 2005, prior to being charged with any wrongdoing, Mr. Epstein retained Roy Black, Esq., to represent him in connection with the then ongoing state investigation. Black Aff. ¶3. Mr. Black in turn hired [REDACTED] of [REDACTED] a private investigation firm, to assist him in his representation of Mr. Epstein. Black Aff. ¶4.

During the course of the state investigation, law enforcement authorities concluded that at some time, one or more computers had been removed from Mr. Epstein's home by a private investigator working at the instruction of Mr.

Epstein's counsel. It is those computers;<sup>1</sup> the testimony of the private investigator; and documents relating to the retention and to the work-product of the investigator that are sought by the subpoenas.

Both prior to the charge being brought and thereafter defense counsel were provided with open disclosure of the state's evidence. Black Aff. ¶6. As a result, all or virtually all of the evidence obtained by the state in its investigation has been reviewed by the defense. *Id.* Included in the materials reviewed are the audio and/or video taped sworn statements of 18 witnesses, transcripts of all 18 of those recorded sworn statements, the transcript of one additional sworn statement, and over 125 pages of documents prepared by the Palm Beach Police Department which detail *every* sworn statement obtained by detectives, *every* interview conducted by detectives, all their investigative efforts, and all the evidence gathered. *Id.* These documents include the entire police file, as well as the probable cause affidavits prepared by Palm Beach detectives and the application for a search warrant of Mr. Epstein's home. *Id.* Reviewing these materials has afforded the defense with a thorough understanding of the factual bases for any allegations that have been, or could have been, made against Mr. Epstein. Black Aff. ¶7.

---

<sup>1</sup> We do not concede the existence of any such computers. However, for purposes of this motion, we refer herein to "computers" as if one or more computers described in the subpoenas do exist.

In approximately January 2007, a grand jury in the Southern District of Florida initiated what was termed a "parallel" investigation to determine whether the conduct in which Mr. Epstein had allegedly engaged violated federal laws, including violations of 18 U.S.C. §2423 (travel for the purpose of engaging in unlawful sexual activity); and 18 U.S.C. §2422(b), use of the internet or other means of interstate communication to persuade, entice or coerce another to engage in unlawful sexual activity. Black Aff. ¶¶8, 11. We understood the conduct being scrutinized by the federal grand jury was the same as the subject of the state prosecution. Black Aff. ¶8. Indeed, during the course of the federal investigation, prosecutors asked for and were provided with copies of the 18 recorded sworn witness statements, and further asked for copies of the transcripts of those sworn statements. *Id.*

That the two investigations examine the same alleged conduct is also clear from Palm Beach Police Chief [REDACTED] [REDACTED] letter expressing the Department's displeasure with the actions of the state grand jury and State Attorney's Office, and explaining he was referring the matter to federal authorities in order to initiate a federal investigation of the facts. Black Aff. ¶9, *see also* Black Aff. Exhibit "B". At the same time, the Palm Beach Police Department both publicly released copies of its files, including the 87 page police report and

probable cause affidavits prepared by its detectives, and publicly announced its intentions to bring the investigation to federal authorities due to the Department's dissatisfaction with the State Attorney's handling of the matter. Black Aff. ¶9, *see also* Black Aff. Exhibit "C".

The discovery provided by state authorities in connection with the state prosecution disclosed no allegations or evidence of use of the internet, e-mail or computer based pornography or any other way in which a computer could be used to commit any of the crimes under investigation. Black Aff. ¶12. Nor, did the numerous discussions with federal prosecutors regarding the federal grand jury investigation reveal any such evidence. Black Aff. ¶¶10, 12, 13.

These subpoenas were not issued in a vacuum. They are simply the most recent of a series of highly intrusive and unusual attempts to acquire highly personal and/or privileged information concerning Mr. Epstein that can have no relevance whatever to the investigation, including Mr. Epstein's personal tax returns, medical records including treatment notes of Mr. Epstein's treatment by a chiropractor, and now, invasion of the defense camp by seeking records of the investigative work performed by [REDACTED] on behalf of Mr. Epstein's counsel in the very same investigation.

The attempt to compel the production of an investigator's "records of dates of communication with Mr. Epstein (or with a third party on Mr. Epstein's behalf)" and to compel the production of records of investigative work "performed on behalf of Mr. Epstein" is an extraordinary invasion of the defense team representing Mr. Epstein as both an indicted state criminal defendant and as a target of the current federal investigation.

While the propriety of those other subpoenas is not at issue here, the subpoenas to [REDACTED] and to his firm are. When it was pointed out to prosecutors that internal Department of Justice rules require, *inter-alia*, that issuance of the subpoenas be predicated on the pre-approval of the Assistant Attorney General of the Criminal Division under the United States Attorneys' Manual ("USAM"), §9-11.255, the question as to whether such approval had been obtained was simply ducked in an unilluminating exchange of correspondence. Though such guidelines create no third party rights, the fact that the required approval evidently was not obtained highlights the continuing overreaching of this investigation.

Moreover, quite apart from whether the required steps were taken internally to obtain approval before issuing the subpoenas, as a substantive matter, the government could not meet the internal guidelines necessary for issuing a subpoena seeking information relating to the representation of a client set forth in

USAM §9-13.410, including that “the information sought [be] reasonably needed for the successful completion of the investigation.”

The challenged subpoenas call for the production, without limitation, of the entire contents of these computers. *See* Black Aff. Exhibit “A”. Assuming the computers exist, they can be presumed to contain a vast array of data and documents, private and business related, none of which has been shown at any time to be of any relevance whatever to the investigation. They would also contain information and documents protected by the attorney-client and work-product privileges. Black Aff. ¶15. Compliance with the subpoenas would therefore necessarily require Mr. Epstein, through the agent of his attorney, to open all aspects of his life to government inspection and leave the government free to rummage at will through privileged, private, and business materials which are wholly irrelevant and unrelated to the subject matter of the government’s investigation.<sup>2</sup>

First, compliance with the subpoenas by Mr. [REDACTED] and/or his firm would violate Mr. Epstein’s Fifth Amendment rights because the act of production would,

---

<sup>2</sup> Even a single computer of the type in standard home usage can contain a volume of information many orders of magnitude greater than the paper storage capacity of a normal home. For example, hard drives sold in 2005 “generally have storage capacities of about eighty gigabytes, roughly the equivalent of *forty million pages of text* – about the information contained in the books on one floor of a typical academic library.” *United States v. Vilar*, 2007 WL 1075041 at \*35 (S.D.N.Y. April 4, 2007) (emphasis added); accord *In re Search of Premises Known as 1406 N. 2nd Ave.*, 2006 WL 709036 at \*3 (W.D. Mich. March 17, 2006) (home computer can easily hold 40,000 books); see also *In re Search of 3817 W. West End*, 321 F. Supp.2d 953, 959 (N.D. Ill. 2004).

under the teaching of *Fisher v. United States*, 425 U.S. 391, 398 (1976), result in compelling testimony from Mr. Epstein himself, in violation of his right against self incrimination. Further, it would also result in invasion of the defense camp, not only questioning actions taken by counsel to Mr. Epstein, but seeking the production of materials to which the government has no possible claim of right – materials protected by Mr. Epstein’s attorney-client and work product privileges. Black Aff. ¶15.

Moreover, it is simply beyond dispute that no court would uphold a subpoena that purports to require a person to produce every letter, every document, every bill, every record, every book, every photograph, every page from a magazine or newspaper he ever snipped, and every message he ever wrote, in other words, every piece of paper that is or has ever been in his home, without limitation or particularization. Yet, that is in effect what these subpoenas seek. For this reason alone, the subpoenas are *per se* unreasonable under the Fourth Amendment, the Due Process Clause of the Fifth Amendment, and Fed.R.Crim.P. Rule 17(c); and should be quashed in their entirety.

Indeed, the fact that there are so many ways in which the subpoenas violate Mr. Epstein’s fundamental rights may well be underscored by the fact that the government has failed to comply wither procedurally or substantively with the

directives of the Department of Justice regarding issuance of subpoenas calling for information relating to legal representation.

Even if the Court determines that the computers themselves must be produced pursuant to the grand jury subpoenas, compelled production does not overcome the need for the government both to particularize a subpoena and further to demonstrate probable cause to search any particular folder or file that is part of the contents of the computer. Until and unless there is a demonstration that probable cause exists to search for and seize particular documents, no search should be permitted.

**I. MR. EPSTEIN IS ENTITLED TO INTERVENTION AS A MATTER OF RIGHT.**

Fed. R. Civ. P. 24(a) grants intervention as a matter of right

. . . when the applicant claims an interest relating to the property or transaction which is the subject of the action and the applicant is so situated that the disposition of the action may as a practical matter impair or impede the applicant's ability to protect that interest, unless the applicant's interest is adequately represented by existing parties.

Mr. Epstein's interests in protecting materials encompassed within his attorney-client and work-product privileges; in preventing the use against him of compelled testimony in violation of his Fifth Amendment rights; and in protecting his

personal and business documents from wholesale invasion by the government amply satisfy this standard.

Intervention as of right under Fed.R.Civ.P. Rule 24(a)(2) must be granted if it is determined that

(1) the application to intervene is timely; (2) the applicant has an interest relating to the property or transaction which is the subject of the action; (3) the applicant is so situated that the disposition of the action, as a practical matter, may impede or impair his ability to protect that interest; and (4) the applicant's interest will not be represented adequately by the existing parties to the suit.

*Sierra Club v. Leavitt*, 2007 WL 1649987 at \*3 (11<sup>th</sup> Cir. June 8, 2007), quoting *ManaSota-88, Inc. v. Tidwell*, 896 F.2d 1318, 1321 (11<sup>th</sup> Cir. 1990). As detailed below, all four requirements are amply met here.

First, the application is timely, as it is being filed prior to enforcement of the subpoenas. Second, Mr. Epstein plainly has a significant interest in protecting his attorney-client and work-product privileges, in asserting his Fifth Amendment privilege, and in preventing unwarranted government rummaging through the contents of his computers. Third, litigation concerning the enforceability of the subpoenas without Mr. Epstein's participation in the proceedings would leave him powerless to protect these vital interests. Fourth, these interests are personal to him and cannot be represented adequately by either the government or [REDACTED].

Accordingly, Mr. Epstein should be afforded the right to intervene in this matter.

**II. MR. EPSTEIN'S ACT-OF-PRODUCTION PRIVILEGE PRECLUDES THE GOVERNMENT FROM COMPELLING MR. RILEY TO PRODUCE THE ITEMS AT ISSUE.**

Compelled production of the items demanded by the subpoenas would violate Mr. Epstein's right, guaranteed by the Fifth Amendment, not to be compelled to be a witness against himself. Because of the clear testimonial aspects that compliance with the subpoenas would require, the "act-of-production" privilege precludes the government from demanding that [REDACTED] appear and produce these items.

The Fifth Amendment "protects a person from being compelled to be a witness against himself". *Fisher v. United States*, 425 U.S. at 398. The privilege extends beyond oral testimony to embrace all compelled testimonial communications that are potentially incriminating. It specifically includes the act of producing documents where such production itself "communicates" information. *See Fisher*, 425 U.S. at 408. As the Supreme Court put it: "[a]lthough the contents of a document may not be privileged, the act of producing the document may be" because "[a] government subpoena compels the holder of the document to perform an act that may have testimonial aspects and an

incriminating effect”. *United States v. Doe*, 465 U.S. 605, 612 (1984); *see also Fisher*, 425 U.S. at 410 (“the act of producing evidence in response to a subpoena . . . has communicative aspects of its own, wholly aside from the contents of the papers produced”). This is so because

[c]ompliance with the subpoena tacitly concedes the existence of the papers demanded and their possession or control by the [subpoenaed party]. It would also indicate the [subpoenaed party’s] belief that the papers are those described in the subpoena.

*Doe*, 465 U.S. at 612, *quoting Fisher*, 425 U.S. at 410; *see also United States v. Hubbell*, 530 U.S. 27, 40 (2000) (compelled testimony “is not to be found in the documents produced in response to the subpoena” but is instead “the testimony inherent in the act of producing those documents”); *In re Grand Jury Subpoena*, 87 F.3d 1198, 1200 (11<sup>th</sup> Cir. 1996) (“[t]he production of documents conveys the fact that the documents exist, that they were in the possession of the witness, and that they were the documents subject to the subpoena. . . . Where these communicative acts of production have ‘testimonial’ value and incriminate the witness, the Fifth Amendment privilege may be invoked”); *accord United States v. Argomaniz*, 925 F.2d 1349, 1355-56 (11<sup>th</sup> Cir. 1991) (by producing the documents called for under the subpoena, the defendant “would be establishing the existence and authenticity of the documents listed in the summons, as well as verifying that these documents

were in his possession”); *In re Grand Jury Subpoena dated April 9, 1996*, 87 F.3d 1198, 1200 (11<sup>th</sup> Cir. 1996); *United States v. Gecas*, 50 F.3d 1549, 1566 (11<sup>th</sup> Cir. 1995); *In re Grand Jury Subpoena Duces Tecum*, 754 F.2d 918, 921 (11th Cir. 1985) (“the act of production alone can constitute self-incriminating testimony”); *In re Grand Jury 83-8*, 611 F. Supp. 16, 21 (S.D. Fla. 1985) (“the act of producing evidence in response to a subpoena . . . does have testimonial aspects of its own, wholly apart from the contents of the papers produced”); *In re Keller Financial Services of Florida, Inc.*; 258 B.R. 391, 403 (M.D. Fla. 2000); *Federal Savings & Loan Ins. Corp. v. Hardee*, 686 F. Supp 885, 887 (N.D. Fla. 1988).

Had the subpoenas been served directly on Mr. Epstein and demanded that he produce the items which had at some point allegedly been in his Palm Beach home or had ever belonged to him, Mr. Epstein would unquestionably be entitled to the protection of the act-of-production privilege. That is so because, as noted above, production thereof would inherently admit that the materials exist and that they had been in his home and/or belonged to him, which would, in turn, at a minimum, implicitly authenticate the contents of the materials. *See, e.g., United States v. Stewart*, 2003 WL 23024461 at \*3 (S.D.N.Y. December 29, 2003) (act of production privileged where government’s claimed relevance for requiring the defendant to produce the subpoenaed documents “depends on the fact that the

documents were produced by [defendant] from his files; [c]learly such an act of production is testimonial, and may not be compelled”); *United States v. Bell*, 217 F.R.D. 335 (M.D. Pa. 2003) (where government lacks knowledge of specific documents, party’s production of the subpoenaed documents would testify to their existence and his possession of them).

Even if the government is correct in its belief that the items listed in ¶’s 1 and 2 of the subpoenas are presently in the possession of ██████████ and/or his firm, ██████████’s possession of the items would not lessen Mr. Epstein’s right to the protection of the act-of-production privilege. ██████████ is an investigator retained to assist counsel in representing Mr. Epstein in the very matter under investigation by the federal grand jury that issued the subpoenas. As such, ██████████ stands in the same relationship to Mr. Epstein as counsel himself. *See, e.g., Linde Thomson Langworthy Kohn & Van Dyke, P.C. v. Resolutions Trust Corp.*, 5 F.3d 1508, 1514 (D.C.Cir.1993); *In re Bieter Co.*, 16 F.3d 929, 936-38 (8<sup>th</sup> Cir. 1994); *Westinghouse Elec. Corp. v. Republic of Philippines*, 951 F.2d 1414, 1424 (3d Cir. 1991); *United States v. Cote*, 456 F.2d 142, 144 (8<sup>th</sup> Cir. 1972); *United States v. Judson*, 322 F.2d 460, 462 (9<sup>th</sup> Cir. 1963); *United States v. Kovel*, 296 F.2d 918, 922 (2d Cir. 1961); *Burlington Indus. v. Rossville Yarn, Inc.*, No. CIV.A.495-CV-0401-H, 1997 WL 404319, at 3 (N.D. Ga. June 3, 1997); *see also United States v.*

*Schwimmer*, 892 F.2d 237, 243 (2d Cir. 1989). In short, the investigator in turn stands in the shoes of his client. *See Fisher*, 425 U.S. at 404.

Since production of the subpoenaed items by Mr. Epstein's legal team would, therefore, be the equivalent of production by Mr. Epstein, and the testimonial communication inherent in that production is the same as if it were Mr. Epstein himself appearing before the grand jury, the full protection of the act-of-production privilege applies here, and the subpoenas must be quashed in their entirety.

### **III. THE SUBPOENAS VIOLATE MR. EPSTEIN'S RIGHT TO COUNSEL UNDER THE SIXTH AMENDMENT RIGHT TO EFFECTIVE ASSISTANCE OF COUNSEL AS WELL AS THE ATTORNEY-CLIENT AND WORK-PRODUCT PRIVILEGES.**

As drafted, in addition to his Fourth Amendment rights, the subpoenas violate the work-product doctrine, as well as Mr. Epstein's Fifth Amendment right to due process and his Sixth Amendment right to counsel. In *Hickman v. Taylor*, 329 U.S. 495, 510-11 (1947), the Supreme Court recognized the modern work-product doctrine, holding that:

[i]n performing his various duties, however, it is essential that a lawyer work with a certain degree of privacy, free from unnecessary intrusion by opposing parties and their counsel. Proper preparation of a client's case demands that he assemble information, sift what he considers to be the relevant from the irrelevant facts, prepare his legal

theories and plan his strategy without undue and needless interference.

The work-product doctrine grants attorneys “a zone of privacy within which to prepare the client's case and plan strategy, without undue interference”. *In re San Juan Dupont Plaza Hotel Fire Litig.*, 859 F.2d 1007, 1014 (1<sup>st</sup> Cir. 1988). It applies in criminal as well as in civil cases. *United States v. Nobles*, 422 U.S. 225, 236-38 (1975) (“Although the work-product doctrine most frequently is asserted as a bar to discovery in civil litigation, its role in assuring the proper functioning of the criminal justice system is even more vital”).

Equally important, the Supreme Court made it clear in *Nobles* that the work-product doctrine necessarily extends to work performed by an investigator for a defendant's attorney:

At its core, the work-product doctrine shelters the mental processes of the attorney, providing a privileged area within which he can analyze and prepare his client's case. But the doctrine is an intensely practical one, grounded in the realities of litigation in our adversary system. One of those realities is that attorneys often must rely on the assistance of investigators and other agents in the compilation of materials in preparation for trial. It is therefore necessary that the doctrine protect material prepared by agents for the attorney as well as those prepared by the attorney himself.

422 U.S. at 238-39; *see also See Cox v. Administrator U.S. Steel & Carnegie*, 17 F.3d 1386, 1422 (11<sup>th</sup> Cir.), *modified on other grounds*, 30 F.3d 1347 (11<sup>th</sup> Cir.

1994) (documents containing the mental impressions, conclusions, opinions, or other legal theories of an attorney or other representative of a party, concerning the litigation are, absolutely protected).

Clearly, the subpoenas served in this case improperly infringe upon the work-product doctrine. The subpoenas seek production of retainer agreements, employment agreements, records of dates when services were performed and the hours worked, telephone logs or records of dates of communications with Mr. Epstein, appointment calendars and diaries during any period in which work was performed for Mr. Epstein or any communication was had with Mr. Epstein (or with a third party on Mr. Epstein's behalf), and records of fee arrangements and payments received for work performed on Mr. Epstein's behalf. *See* Black Aff. Exhibit "A". These records, which contain evidence of work performed on behalf of Mr. Epstein and his attorneys, must be protected from disclosure by the work-product doctrine.

The government cannot invade the defense camp through the mechanism of a subpoena any more than it can by the surreptitious planting of an informant. *See, e.g., United States v. Henry*, 447 U.S. 264, 266 (1980) (rule in *Massiah v. United States*, 377 US. 201 (1964), violated when law enforcement agent instructed jailhouse informant "to be alert" for any incriminating statements). Nor can it do

so by keeping note of the documents selected by defense counsel for copying during the discovery process. *United States v. Horn*, 811 F.Supp.739 (D.N.H. 1992).<sup>3</sup> In *Horn*, government counsel instructed an agent to make two copies of every document selected by defense counsel to be copied from amongst the materials made available for inspection by the government during the discovery process, and then used the documents to prepare a government witness, even after defense counsel objected to the copying and while a motion to seal the materials was pending. *Horn*, 811 F.Supp. at 748-749. Concluding that “there is every indication that the lead prosecutor wanted to . . . obtain an insight into defense counsel’s trial strategy, tactics, and thought processes without any concern for the rights of the defendants,” *Horn*, 811 F.Supp. at 749, the court found that the government had violated defendants’ work-product privilege, as well as their Fifth Amendment right to due process and their Sixth Amendment right to effective assistance of counsel. 811 F.Supp. at 752; *see also United States v. Horn*, 29 F.3d 754, 758 (1<sup>st</sup> Cir. 1994) (in government’s appeal of one of the district court’s remedies — ordering the government to pay defense legal fees to litigate the issue — the Court noted that the district court “ruled that this prosecutorial misconduct

---

<sup>3</sup> As the court in *Horn* noted, several courts have held that defense counsel’s selection and compilation of documents in preparation for pretrial discovery fall within the highly-protected category of opinion work product. *Shelton v. American Motors Corp.*, 805 F.2d 1323, 1329 (8th Cir. 1986); *Sporck v. Peil*, 759 F.2d 312, 315-16 (3d Cir. 1985); *United States v. District Council of New York City and Vicinity of the United Bhd. of Carpenters and Joiners of Am.*, 1992 WL 208284 at \*12 (S.D.N.Y. Aug. 18, 1992); *James Julian, Inc. v. Raytheon Co.*, 93 F.R.D. 138, 144 (D. Del. 1982).

not only violated the defendants' work-product privilege, but also abridged their Fifth Amendment right to due process and their Sixth Amendment right to effective assistance of counsel"); accord *United States v. Marshank*, 777 F.Supp. 1507, 1519 (N.D. Cal. 1991) (“[w]hen the government interferes in a defendant's relationship with his attorney to the degree that counsel's assistance is rendered ineffective, the government's misconduct may violate the defendant's Fifth Amendment right to due process as well as his Sixth Amendment right to counsel”).

The subpoenas at issue here are akin to the conduct condemned in *Horn*. Here, through the issuance of a subpoena, the government seeks to track the investigation being conducted at the direction and under the supervision of his attorneys in an effort to obtain insight into defense counsel's strategy, tactics, and thought processes, without any concern for the rights of Mr. Epstein. Permitting the government to do so would violate the work-product privilege, Mr. Epstein's Fifth Amendment right to due process and his Sixth Amendment right to effective assistance of counsel.<sup>4</sup>

Indeed, many of the ways in which the subpoenas at issue trample on Mr. Epstein's rights are the very problems sought to be avoided by the internal

---

<sup>4</sup> State proceedings were commenced against Mr. Epstein on July 17, 2006. Black Aff. ¶5. It is well established that an individual's Sixth Amendment right to counsel attaches once prosecution is commenced. See, e.g., *Texas v. Cobb*, 532 U.S. 162, 167 (2001) (Sixth Amendment right to counsel attaches once prosecution is commenced).

Department of Justice guidelines for the issuance of subpoenas seeking information relating to legal representation. As demonstrated above, a subpoena to a defense investigator under these circumstances is the same as a subpoena to defense counsel. And USAM Guideline §9-11.255 requires prior Department of Justice approval for the issuance of a subpoena to a lawyer. That requirement evidently was not met. *See* Black Aff. ¶15. Second, “because of the potential effects upon an attorney-client relationship that may result from the issuance of a subpoena for information relating to the attorney’s representation of a client”, the DOJ imposes strict requirements on such issuance. Among the requirements that must be met is that “there must be reasonable grounds to believe that . . . the information sought is reasonably needed for the successful completion of the investigation or prosecution. The subpoena must not be used to obtain peripheral or speculative information”. USAM §9-13.410. Though these guidelines create no enforceable rights, the prosecutors’ failure here to comply with the internal requirements provide further evidence that these subpoenas are an inappropriate and unwarranted attempt to invade Mr. Epstein’s defense camp.

**IV. THE SUBPOENAS ARE UNREASONABLE IN THAT IT SEEKS PRODUCTION OF THINGS UNCONNECTED TO ANY CRIME UNDER INVESTIGATION.**

This Court has authority to review a grand jury subpoena for reasonableness. *See, e.g., United States v. R. Enterprises, Inc.*, 498 U.S. 292, 300-01 (1991). While the Supreme Court has held that grand jury subpoenas are presumed reasonable, that presumption may be overcome and a subpoena quashed where, as here, “there is no reasonable possibility that the category of materials the [g]overnment seeks will produce information relevant to the general subject of the grand jury’s investigation”. *R. Enterprises, Inc.*, 498 U.S. at 301. Normally, as the Supreme Court noted in *R. Enterprises, Inc.*, recipients of a grand jury subpoena have little or no knowledge of the crime the grand jury is investigating and will therefore be unable to challenge the issuance of the subpoena on reasonableness grounds. *Id.* at 301-02. Here, that is not the case. Mr. Epstein is aware not only of the subject matter, but the exact charges the grand jury is investigating. *See* Black Aff. ¶11. From that, it is clear that the evidence the government is attempting to obtain is wholly irrelevant to the grand jury’s investigation. *See Id.* ¶¶12, 13.

The requirement that a grand jury subpoena be reasonable and particularized is beyond dispute. Not only is that explicitly stated in the Fourth Amendment, but

the requirement is included in Fed. R. Crim. P. Rule 17(c). *See, e.g., R. Enterprises*, 498 U.S. at 299 (Rule 17(c) requires that grand jury subpoenas be reasonable); *United States v. Dionisio*, 410 U.S. 1, 11 (1973) (“[t]he Fourth Amendment provides protection against a grand jury subpoena *duces tecum* too sweeping in its terms to be regarded as reasonable”); *Oklahoma Press Pub. Co. v. Walling*, 327 U.S. 186, 208-09 (1946) (holding that subpoenas although not searches and seizures under the Fourth Amendment, must be reasonable). Subpoenas, such as the ones here, which are overbroad and lack particularity such that they sweep within their scope a multitude of irrelevant documents is quintessentially unreasonable, whether assessed under the Fourth Amendment, the Due Process Clause, or Rule 17(c).

Grand juries “are not licensed to engage in arbitrary fishing expeditions”. *R. Enterprises, Inc.*, 498 U.S. at 299. Yet that is precisely what enforcement of these subpoenas would permit – unbridled rummaging by the government through an individual’s “papers and effects” – namely, the contents of computers with no restriction or aim other than to “find something” of which the government has no evidence whatever exists. That renders these subpoenas the equivalent of a general search – the very evil that the Fourth Amendment was crafted to prohibit.

In its Requests at ¶1's and 2, rather than making any effort to limit the subpoenas to matters relevant to its investigation (which we submit could not here be done), the government instead improperly seeks the entire contents of the computers, despite no evidence they contain any documents of any conceivable relevance to the government's investigation. *See* Black Aff. Exhibit "A". Such a subpoena is unreasonable and overbroad in violation of the Fourth Amendment, the Due Process Clause, and Rule 17(c).

Similarly, the materials listed in ¶3 are fundamentally irrelevant to the government's investigation of Mr. Epstein, which is focused on allegations of sexual activity with underage girls. Neither Mr. Epstein's communications with his retained investigator, Mr. Riley (or his firm), nor any services Riley and his firm may have performed on behalf of Mr. Epstein, has any possible bearing on the government's investigation. Moreover, as demonstrated in Point III, *supra*, enforcement of the subpoenas as to ¶3 poses a grave threat to Mr. Epstein's Sixth Amendment right to counsel and to his attorney-client and work-product privileges.

For instance, certain of the materials requested in ¶3, such as the Requests for "information related to the nature of the relationship between [REDACTED] and/or [REDACTED] and Mr. Jeffrey Epstein" (Black Aff. Exhibit "A"), on

their face clearly implicate the work-product privilege; other Requests, such as those seeking billing records and records of services provided to Mr. Epstein, (*id.*), would require the redaction of work-product if the government were to be permitted access to them at all, given their irrelevance to the investigation. Since there is no issue as to Mr. Epstein's wealth or the source of the funds used to pay for the services, that irrelevance also extends to the requested documents showing the fees Mr. Epstein may have paid to [REDACTED] for its services, as well.

**V. EVEN IF THE GOVERNMENT IS PERMITTED TO SEIZE THE COMPUTERS ON THE BASIS OF A GRAND JURY SUBPOENA, THE SUBPOENAS MUST BE QUASHED AS UNREASONABLE AND OPPRESSIVE, OVERBROAD AND UNPARTICULARIZED.**

Paragraphs 1 and 2 of the subpoenas suggest no limitation on the ability of the government to search the contents of the computers. Instead, the government purports to be able to read and to maintain in its possession every bit of data stored therein, with no limit as to subject matter or time frame. Quite clearly, the subpoenas are intended to allow the government to "go fishing" in the computers. In fact, the government has no reasonable basis for a belief that any information contained within the computers would be relevant to its investigation. *See* Black Aff. ¶12. Thus, Request ¶'s 1 and 2 cannot, consistent with the requirements of the Fourth Amendment and the protections against unreasonable subpoenas afforded by Rule 17(c), be enforced. Instead, the intervention of the Court is required to

prevent the government from using a grand jury subpoena to conduct an unfettered general search of the contents of the computers. See *United States v. Comprehensive Drug Testing, Inc.*, 473 F.3d 915, 938-39 (9<sup>th</sup> Cir. 2006) (“[i]t is not reasonable to allow the government to seize an indeterminately bounded array of computer data only later to set its own standards for review and retention thereof”).

Further, where that which the government seeks is not the computers themselves but rather the *content* of the computers, it is that content which must be particularly described in the subpoena to comply with the reasonableness requirement. See *In re Grand Jury Subpoena Duces Tecum Dated November 15, 1993*, 846 F.2d 11, 13 (S.D.N.Y. 1994). The subpoenas at issue fail utterly to do so. Rather, they are overbroad and unparticularized, and as such, cannot pass muster under either the Fourth Amendment or Rule 17(c).

The “reasonableness” requirement is understood to contemplate a requirement that the subpoena identify with particularity the documents to be produced. *Fisher*, 425 U.S. at 401 (Fourth Amendment protects against subpoenas which suffer from “too much indefiniteness or breadth in the things required to be particularly described”); *Oklahoma Press*, 327 U.S. at 209 (“the requirement is reasonableness, including particularity in describing the place to be searched and

the persons or things to be seized”). Here, though the subpoenas describe with particularity “the computers”, the subpoenas are wholly silent as to the real target – the *contents* of the computers. As courts have recognized in the context of search warrants authorizing searches of computers, the particularity requirement cannot be deemed satisfied absent specification of the documents or other materials which are the object of the search/subpoena.

Courts are increasingly recognizing that careful attention to the Fourth Amendment’s particularity requirement and overbreadth prohibition are critical in the context of computer searches. *See, e.g., United States v. Adjani*, 452 F.3d 1140, 1149 (9<sup>th</sup> Cir. 2006) (“[w]e understand the heightened specificity concerns in the computer context, given the vast amounts of data they can store”); *In re Search of 3817 W. West End*, 321 F.Supp.2d at 958-59 (marshalling the reasons why “a request for the search and seizure of computers merits a close look at the particularity requirement”); *see also* U.S. Dep’t of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (July 2002) (“DOJ Computer Search Manual”) (“[a]gents must take special care when describing the computer files or hardware to be seized”).

Courts have held that “when the government seeks to seize the information stored on a computer, as opposed to the computer itself, that underlying

information must be identified with particularity and its seizure independently supported by probable cause”. *United States v. Vilar*, 2007 WL 1075041 at \*36; *United States v. Riccardi*, 405 F.3d 852, 862 (10<sup>th</sup> Cir. 2005) (“warrants for computer searches must affirmatively limit the search to evidence of specific federal crimes or specific types of material”); *United States v. Barbuto*, 2001 WL 670930 at \*5 (D.Utah April 12, 2001) (agents “should have known that the warrant needed to specify what types of files were sought in the searching of the two computers so that personal files would not be searched); *see also* DOJ Computer Search Manual at 42 (instructing that “[i]f the probable cause relates only to the information . . . the warrant should describe the information, rather than the physical storage devices which happen to contain it”). Thus, “[t]o withstand an overbreadth challenge, the search warrant itself, or materials incorporated by reference must have specified the purpose for which the computers were seized and delineated the limits of their subsequent search”. *United States v. Hunter*, 13 F.Supp.2d 574, 584 (D.Vt. 1998)

Given these principles, the Requests contained in ¶’s 1 and 2 of the subpoenas are clearly unreasonable, since they purport to allow the government to search the entire contents of the computers with no requirement of showing reasonableness or relevance to the matters under investigation. That is not

permissible. *See, e.g., Riccardi*, 405 F.3d at 862-63 (warrant authorizing seizure of computer, all electronic and magnetic media stored therein, and a host of external storage devices without limitation unconstitutional as authorizing general search); *United States v. Joe*, 2007 WL 108465 at \*7 (N.D.Cal. January 10, 2007) (holding “computers and related or similar devices, and information on hard or floppy drives, which may contain any documents and records . . . .” overbroad and ordering suppression); *United States v. Slaey*, 433 F.Supp.2d 499, 500 (E.D. Pa. 2006) (“[a]ny records, documents, materials and files maintained on a computer” overbroad because it authorized agents to seize everything, even if unrelated to the offense under investigation and even if wholly personal); *West End*, 321 F.Supp.2d at 962 (refusing to approve unguided search, which the government indicated could require review of all the seized data, because “what the government seeks is a license to roam through everything in the computer without limitation and without standards”); *United States v. Clough*, 246 F.Supp.2d 84, 87-88 (D. Me. 2003) (warrant to search computers which contained no limitations on the search and no references to statutes, crimes, or illegality was unconstitutionally overbroad); *Hunter*, 13 F.Supp.2d at 584 (warrant authorizing seizure of all computers, all computer storage devices, and all computer software systems unconstitutionally overbroad).

Where, as here, computers or their contents or external storage media and devices are sought to be hauled away by the government for later off-site search, courts have an obligation to ensure that the subsequent search remains within the bounds of the Fourth Amendment reasonableness requirement. “[R]esponsible officials, *including judicial officers*, must take care to assure that [searches] are conducted in a manner that minimizes unwarranted intrusions upon privacy”. *West End*, 321 F.Supp.2d at 960, *quoting Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976).

Most recently, in *Warshak v. United States*, 2007 WL 1730094 (6<sup>th</sup> Cir. June 18, 2007), the Sixth Circuit, in the context of upholding a Fourth Amendment challenge to the provisions of the Stored Communications Act which authorize the government to obtain an individual’s emails from his Internet Service Provider pursuant to court order or subpoena on a showing of less than probable cause and without advance notice to the subscriber, expressly addressed the particularity requirement where subpoenas as well as searches of computers are concerned:

Because our opinion speaks to the appropriate remedy in this case, we note one other important principle that applies both to e-mail seizures pursuant to a warrant supported by probable cause, and to compelled disclosure through a process akin to that involved with subpoenas. In neither instance is the government necessarily entitled to every e-mail stored with the ISP, many of which are likely to be entirely unrelated to its specific investigation . . . where a subpoena . . . compels the disclosure of e-

mails, the demand must be reasonable in scope and relevance.

*Id.* at 15 n.8 (citations omitted).

Similarly, the court in *In re Grand Jury Subpoena Duces Tecum Dated November 15, 1993*, *supra*, 846 F.2d 11, was called upon to review a grand jury subpoena that sought all computer hard drives of computers supplied to a number of officers and employees or a corporate entity, as well as all computer-accessible data, including all floppy disks, created by or on behalf of the specified officers or employees. The Court held that, because there were ways in which the government could have narrowed the subpoena to relevant documents, such as documents containing certain key words, the subpoena at issue unnecessarily demanded documents irrelevant to the grand jury inquiry and was, therefore, unreasonably broad under Rule 17. Likewise, in *In re Amato*, 2005 WL 1429743 at \*11-\*12 (D. Me. June 17, 2005), the Court, relying on a number of cases dealing with searches of computers pursuant to warrants, granted a motion to quash with respect to the paragraph of the subpoena requesting the production of all computers and computer related equipment: "Inasmuch as Category 10 of the Subpoenas in essence requests the turnover of all computers (and related objects) of both corporations with no express safeguard against a subsequent rummaging through,

and seizure of, irrelevant as well as relevant data, it cannot withstand Fourth Amendment reasonableness scrutiny”.

Courts are now recognizing that the seizure of a computer for later off-site search of its contents requires fresh thinking, and cannot simply be permitted by reference to the law that permits seizure of a file cabinet or other container of physical documents. *See, e.g., United States v. Hill*, 459 F.3d 966, 968 (9<sup>th</sup> Cir. 2006) (“computer-related searches can raise difficult Fourth Amendment issues different from those encountered when searching paper files”); *United States v. Walser*, 275 F.3d 981, 986 (10<sup>th</sup> Cir. 2001) (“[b]ecause computers can hold so much information touching on many different areas of a person’s life, there is a greater potential for the “intermingling” of documents and a consequent invasion of privacy when police execute a search for evidence on a computer”); *United States v. Campos*, 221 F.3d 1143, 1148 (10<sup>th</sup> Cir. 2000) (storage capacity of computers may require law enforcement officers to take a special approach because of intermingled documents); *West End*, 321 F.Supp.2d at 959 (“[t]he capacity of the computer to store these large quantities of information increases the risk that many of the intermingled documents will have nothing to do with the alleged criminal activity that creates probable cause for the seizure”); *Hunter*, 13 F.Supp.2d at 583 (“[c]omputer searches present the same problem as document

searches – the intermingling of relevant and irrelevant material – but to a heightened degree”).

Recently, the Ninth Circuit expressly applied the principles of in *United States v. Tamura*, 694 F.2d 591 (9<sup>th</sup> Cir. 1982), a leading case on the Fourth Amendment issues presented by intermingled documents in the traditional paper document search context,<sup>5</sup> in the computer context, noting that because “the computer era adds new complexity to the test of reasonableness under the Fourth Amendment”, it viewed *Tamura* “as especially important in the computer context”. *United States v. Comprehensive Drug Testing, Inc.*, 473 F.3d 915, 939 (9<sup>th</sup> Cir. 2006). The review procedure outlined in *Tamura* was, the Court concluded, “necessary to ensure that the seizure of intermingled computer records remains reasonable”. *Id.* at 938. Therefore,

. . . in the case of a lawful and reasonable seizure of intermingled computer records for off-site review . . . our precedents and the general reasonableness mandate of the Fourth Amendment require the supervision of a magistrate. *It is not reasonable to allow the government to seize an*

---

<sup>5</sup> In *Tamura*, the Court suggested that where documents are so intermingled that they cannot be feasibly sorted on site, agents “generally can avoid violating Fourth Amendment rights by sealing and holding the documents pending approval by a magistrate of a further search, in accordance with the procedures set forth in the American Law Institute’s Model Code of Pre-Arrest Procedure”. 694 F.2d at 595-96. In fact, the Court continued, if the officers are aware prior to the search that there will be a need to transport documents to another location for search, they should apply to the magistrate for specific approval of large-scale removal of material, which should be granted by the magistrate “only where on-site sorting is infeasible and no other practical alternative exists”. *Id.* at 596. The “essential safeguard” required, the Court stated, is “that *wholesale removal must be monitored by the judgment of a neutral, detached magistrate*”. *Id.* (emphasis added)

*indeterminately bounded array of computer data only later to set its own standards for review and retention thereof.*

*Id.* (emphasis added).

There is no question that Mr. Epstein has an important expectation of privacy in the contents of the subpoenaed materials. Amongst other safeguards, the Fourth Amendment protects Mr. Epstein's privacy absent probable cause that any particularized file or document contains evidence of a federal crime. The issuance of a subpoena does not eliminate the necessity of probable cause when the objects of the compulsion are documents in which a citizen has an expectation of privacy. In cases where the objects of a subpoena are business records, such as bank records in which a citizen has no expectation of privacy (*see, e.g., United States v. Miller*, 425 U.S. 435 (1976)), or telephone toll records (*Smith v. Maryland*, 442 U.S. 735, 740 n. 5 (1979)), a subpoena is sufficient. In cases, however, where an expectation of privacy exists, a subpoena lacking probable cause does not accord with Fourth Amendment rights. *See, generally, Katz v. United States*, 389 U.S. 347 (1967).

For these reasons, to the extent the subpoenas purport to permit the grand jury not only to seize, but to search the computers, they are unreasonable. Before the government may be permitted to search the computers, it must particularize the

items to be seized after a demonstration of probable cause to believe that the computers contain such items.

**VI. THE COURT MUST ENSURE THAT THE GOVERNMENT IS NOT PERMITTED ACCESS TO MATERIALS PROTECTED BY THE ATTORNEY-CLIENT OR WORK-PRODUCT PRIVILEGES.**

Though we believe the subpoenas should be quashed in their entirety, in the event the Court determines to enforce the subpoenas, the Court should be particularly careful to assure that safeguards are put in place to prevent the disclosure of attorney-client communications and attorney work-product. The subpoenaed materials contain information and documents protected by the attorney-client and work-product privileges, including attorney-client communications between Mr. Epstein and attorneys regarding various legal matters with respect to which he sought and obtained the assistance of counsel. Black Aff. ¶13. Prior to any production of the subpoenaed computers, counsel must be permitted to review an image of their contents for the purpose of identifying all privileged materials contained in the computers, segregating the privileged materials from the remaining content of the computers to ensure that privileged materials do not fall into the hands of government investigators.

The Sixth Circuit recently adopted a similar procedure in the context of traditional subpoenaed documents. The Court in *In re Grand Jury Subpoena*, 454 F.3d 511 (6<sup>th</sup> Cir. 2006), was called upon to “determine who has the right to

conduct a review for privilege of documents subject to a grand jury subpoena directed to a third party who possesses the documents but has not yet produced them to the government: the targets of the investigation whose rights of privilege are potentially implicated, or the federal government, operating a 'taint team' behind a 'Chinese wall' or protective screen". *Id.* at 512. The district court had rejected the proposal by the targets of the investigation that their counsel review the responsive documents and prepare a privilege log, with disputes to be resolved by the court in favor of first-instance review by a government "taint team". The Court, noting that "grand juries are not empowered to override private rights in all cases", and, in particular, "may not use their investigatory authority to violate a valid privilege" (*id.* at 519), reversed the district court, concluding that the risks to the attorney-client privilege inherent in the government's review of privileged materials were such that the targets should be permitted the opportunity to conduct their own privilege review prior to production. *See id.* at 521-23. Interestingly, in that case, the government conceded that "the leaking of privileged materials to investigators would raise the specter of *Kastigar*-like evidentiary hearings". *Id.* at 517. This case presents the same specter should Mr. Epstein be indicted.

The recognized importance of the attorney-client privilege is such that this Court should permit Mr. Epstein's counsel to review the contents of the computers to identify all privileged information, segregate it from the remaining contents of

the computers, and create a privilege log. Any disputes regarding privilege should be resolved by the Court prior to access by the government.

**VII. SUBPOENAING PURELY PRIVATE PAPERS VIOLATES THE FIFTH AMENDMENT UNDER *BOYD*.**

In *Boyd v. United States*, 116 U.S. 616 (1886), the Supreme Court condemned the seizure of an individual's private personal papers and their use as evidence against him as violative of the Fifth Amendment. While admittedly *Boyd* has been deeply eroded, and language in *Hubbell*, 530 U.S. at 35-36, would appear to be at odds with this portion of *Boyd*, the relevant portion of *Boyd* pertaining to an individual's private papers has not been directly overruled. Indeed, the Eleventh Circuit, in a case decided pre-*Hubbell*, left open the question of the continued vitality of *Boyd* with respect to personal documents. *In re Grand Jury Investigation*, 921 F.2d 1184, 1187 n.6 (11<sup>th</sup> Cir. 1991). *And see Barrett v. Acevedo*, 169 F.3d 1155, 1167 (8<sup>th</sup> Cir. 1999) ("whether *Doe's* rationale extends to purely personal papers in a defendant's possession is still open to some debate"). Permitting the government to compel an individual to turn over to the government the entire contents of his computers for the government to do with it as it will, including reading all of his most private thoughts and communications, and then using those private writings to try him for a crime, "would break the heart of our

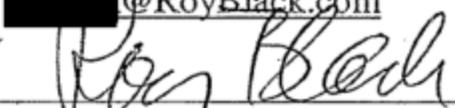
sense of privacy". *In re Steinberg*, 837 F.2d 527, 530 (1st Cir: 1988). It should not be permitted under the Fifth Amendment.

### CONCLUSION

For all these reasons Mr. Epstein's must be permitted to intervyene and to move to quash the subpoena duces tecum issued to [REDACTED], and the motion to quash the subpoenas should be granted in its entirety.

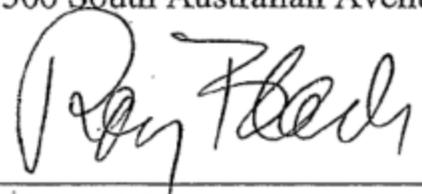
Respectfully submitted,

**BLACK, SREBNICK, KORNSPAN & STUMPF, PA.**  
201 South Biscayne Boulevard, Suite 1300  
Miami, Florida 33131  
Ph.: (305) 371-6421 -- Fax: (305) 358-2006  
E-Mail: [REDACTED]@RoyBlack.com

By:   
\_\_\_\_\_  
ROY BLACK, ESQ.  
Florida Bar No.: 126088  
Counsel for Jeffrey Epstein

### CERTIFICATE OF SERVICE

**I HEREBY CERTIFY** that on July 17, 2007, a true and correct copy of the forging motion was furnished by facsimile (561) 802-1787, and U.S. mail to: Maria Villifana, Esq., U.S. Attorney's Office, 500 South Australian Avenue, Suite 400, West Palm Beach, FL 33401.

By:   
\_\_\_\_\_  
ROY BLACK, ESQ.  
Counsel for Jeffrey Epstein