In re: Grand Jury Subpoena to Sebastien Boucher
United States District Court, District of Vermont
No. 2:06-mj-91
February 19, 2009
Opinion Text

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 in an unencrypted format by opening the drive before the grand jury. (Gov't's Appeal 2.) In oral argument and postargument 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 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 (1991) (de novo review appropriate for §636(b)(3) referral when requested); Mathews v.Weber, 423 U.S. 261, 270 (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 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 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 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 (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 (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 (2000) (quoting Doe v. United States, 487 U.S. 201, 209 (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 (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 (1990) (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 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 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 Judge's opinion and order (Doc. 35) is sustained.

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