UNITED STATES DISTRICT COURT
FOR THE
DISTRICT OF VERMONT

In re: Grand Jury Subpoena to Sebastien Boucher	:	No. 2:06-mj-91

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 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 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 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 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 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 (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 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 (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 control. Doe v. United States, 487 U.S. 201, 209 (1988) [hereinafter Doe II]. The privilege 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 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 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 (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 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 (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 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 (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 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 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 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 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 J. Niedermeier
United States Magistrate Judge

Any party may appeal to this Order within 10 days after service by filing with the clerk of the court and serving on the magistrate judge and all parties, a written statement of appeal which shall specifically designate the order, or part thereof, appealed from and the reason why this order is clearly erroneous or contrary to law. See Local Rule 72.1; 28 U.S.C. § 636(b)(1)(A); Fed. R. Civ. P. 72(a), 6(a) and 6(e).