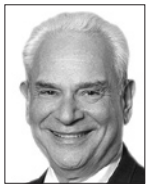
New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 247—NO. 43
TUESDAY, MARCH 6, 2012

WHITE-COLLAR CRIME

Expert Analysis

Passwords, Encrypted Hard Drives, Constitutional Rights and Privileges



By **Elkan Abramowitz**

And **Barry A. Bohrer**

On a number of occasions,this column has examined the evolving case law regarding the application of the Fourth Amendment to digital evidence.[1] A recent case from the U.S. Court of Appeals for the Eleventh Circuit demonstrates that other constitutional protections also may be implicated in the government's seizure of and attempts to search digital evidence. One issue raised by this case, and others like it, is the questionable ability of individuals to protect those rights and privileges in the face of ever-changing technology.

'Act of Production'

In *In re Grand Jury Subpoena Duces Tecum* Dated March 25, 2011,[2] the Eleventh Circuit considered whether the government could compel the defendant, John Doe, to produce the unencrypted contents of his laptop computers and external hard drives that were password-protected. The digital media was lawfully seized during the course of a child pornography investigation. However, because Federal Bureau of Investigation forensic examiners were unable to access certain portions of the hard drives, the defendant was subpoenaed to produce the "unencrypted contents" of the drives.

Doe refused to comply with the subpoena, asserting his Fifth Amendment privilege against self-incrimination. Specifically, Doe contended that his compliance would amount to testimony "that he, as opposed to some other person, placed the contents on the hard drive, encrypted the contents, and could retrieve and examine them whenever he wished."[3] In response, the defendant was granted statutory immunity for the act of production of the unencrypted drives. Noting that the immunity grant did not cover the government's derivative use of the decrypted contents of the drives, Doe persisted in his refusal to comply and was found in contempt.

The circuit court reviewed the district court's findings that: 1) the defendant's decryption and production of the hard drives would not constitute testimony falling within the ambit of the Fifth Amendment's privilege of self-incrimination; and 2) the government was permitted derivative use of the evidence located on the hard drives. Tackling the first question as to whether the defendant's production of the unencrypted contents of the computers was testimonial in nature, the court reviewed two seminal Supreme Court cases and the "spectrum" of law by which to evaluate the testimonial quality of acts of production.

> Significant questions remain regarding the balance between personal privacy and security and law enforcement efforts, particularly in the realm of electronically stored information.

In *Fisher v. United States*, the Supreme Court found that a taxpayer's production to the Internal Revenue Service of voluntarily prepared documents previously provided by the taxpayer to his attorney would not involve testimonial self-incrimination because the authenticity, existence, and location of the papers were a "foregone conclusion and the taxpayer adds little or nothing to the sum total of the [g]overnment's information by conceding that he in fact has the papers."[4] Twenty-four years later, in *United States v. Hubbell*,[5] the Court rejected the application of the "foregone conclusion" doctrine where the government failed to show any prior knowledge of either the existence or whereabouts of the documents subpoenaed from the defendant. In such circumstances, where the government has nothing more than a suspicion that the documents may exist, the production of documents is testimonial in nature and triggers Fifth Amendment protection.

In summary, the Eleventh Circuit observed that the Supreme Court has "marked out two ways in which an act of production is not testimonial." First, where the government merely compels some physical act and the individual is not called upon to make use of the contents of his mind. Second, where under the "foregone conclusion" doctrine, the act of production conveys only a fact regarding the existence, location, possession, or authenticity of the subpoenaed materials that is already known by the government.[6]

In the aforementioned recent case, the Eleventh Circuit found nothing in the record to indicate that the government knew whether any of the files located on Doe's machines contained child pornography or that the government knew "with reasonable particularity that Doe was even capable of accessing the encrypted portions of the drives." Although the government had established the possibility that the drives could contain millions of incriminating files, the court observed that on cross-examination the government's own expert conceded he had no idea whether there was anything other than "random data" on the encrypted drives. Accordingly, the court concluded that the act of production sought by the government was testimonial in character, closer on the spectrum to *Hubbell*.

In reaching its conclusion, the court rejected the government's attempt to analogize the case to two district court opinions in which a defendant had been ordered to produce the unencrypted contents of password-protected hard drives despite assertions of the Fifth Amendment privilege. The Eleventh Circuit noted that in both cases in the district courts the government possessed information indicating that incriminating evidence was located on the hard drives.

In *In re Grand Jury Subpoena to Boucher*,[7] a government agent viewed several images of child pornography after the defendant navigated to the encrypted portion of the hard drive (the Z drive) of

ELKAN ABRAMOWITZ *is a member of Morvillo, Abramowitz, Grand, Iason, Anello & Bohrer and a former chief of the criminal division in the U.S. Attorney's Office for the Southern District of New York.* BARRY A. BOHRER *is a member of Morvillo, Abramowitz and was formerly chief appellate attorney and chief of the major crimes unit in the Southern District U.S. Attorney's Office.* GRETCHAN R. OHLIG, *an attorney, assisted in the preparation of this article.*

his laptop during a secondary border inspection. The defendant was arrested and the laptop seized. Subsequently, the government discovered that it could not open the Z drive without assistance from Sebastien Boucher because it was encrypted and required the entry of a password. Considering Boucher's assertion of the privilege against self-incrimination, the District Court of Vermont found that the foregone conclusion doctrine applied despite the fact that the government had only viewed a few of the files on the Z drive and did not know whether the remainder contained incriminating material.[8]

In *United States v. Fricosu*,[9] a federal District Court for the District of Colorado similarly found that where "[t]here is little question…that the government knows of the existence and location of the computer's files" compelling the defendant to provide access to the computer's unencrypted contents did not violate the privilege.[10] In so finding, the court relied on a tape-recorded conversation in which the defendant essentially admitted that the information being sought by the government was on her laptop. Distinguishing both cases, the Eleventh Circuit stated, "Here, in contrast, the [g]overnment does not know whether any files are present on the encrypted drive; if any, what their location on the drive may be; whether Doe has access and control to the encrypted drives; and whether Doe is capable of decryption."[11] Accordingly, the foregone conclusion doctrine did not apply and the act of producing a decrypted version of the data in Doe's case was deemed testimonial for purposes of Fifth Amendment analysis.

Immunity

Pursuant to statute, an individual can still be compelled to testify despite the protections afforded by the Fifth Amendment privilege against self-incrimination where sufficient immunity—that which is coextensive with the Fifth Amendment—is granted. Section 6002 of Title 18 specifically provides that "no testimony or other information compelled under the order [of immunity] (or any information directly or indirectly derived from such testimony or other information) may be used against the witness in any criminal case, except a prosecution for perjury, giving a false statement, or otherwise failing to comply with the order."

The Eleventh Circuit concluded that the immunity bestowed on Doe by the district court was insufficient under the statute to compel Doe to produce the unencrypted hard drives.[12] Specifically, the court found that the district court erred in limiting Doe's immunity in a manner that permitted the government derivative use of any evidence located on the hard drives. Indeed, the government told the district court that "it would not use Doe's act of production against him in a future prosecution; but it would use the contents of the unencrypted drives against him."[13]

The Eleventh Circuit noted that Supreme Court precedent is clear that use and derivative-use immunity is the critical threshold required to overcome an individual's assertion of the Fifth Amendment. Finding that the government did not meet this threshold, the court rejected the "'manna from heaven' theory, which contended that if the [g]overnment omitted any description of how the documents were obtained, it would be as if they magically appeared on the courthouse steps and the [g]overnment could use the documents themselves."[14] Accordingly, the immunity offered to Doe was not coextensive with the Fifth Amendment and Doe was not compelled to decrypt the drives.

The Fourth Amendment

In 2007, a decision from the U.S. Court of Appeals for the Tenth Circuit examined the impact of encrypted hard drives and password protection of digital evidence in the context of a computer search and seizure. In *United States v. Andrus*,[15] the computer in question was seized from the bedroom of the defendant, Ray Andrus, who was charged with possession of child pornography. The defendant lived with his elderly father, and upon the father's consent, federal authorities conducted a search of Baily Andrus' home, including the defendant's bedroom and his personal computer located on the desk in his bedroom. Using software that allowed them to bypass user profiles and password protection, the federal agents discovered the existence of child pornography on the computer.

The Eleventh Circuit concluded that the immunity bestowed on Doe by the district court was insufficient under the statute to compel Doe to produce the unencrypted hard drives. It found the district court erred in limiting Doe's immunity in a manner that permitted the government derivative use of any evidence located on the hard drives.

Ray Andrus sought to suppress the evidence found on the computer arguing that his father did not have authority to consent to the search, particularly since he did not have a user profile on the computer and did not know the password that would have allowed him to access the contents of the computer. The Tenth Circuit rejected the defendant's argument, finding the search valid under the totality of the circumstances test. The court held that the facts known to the officers at the time the computer search was conducted created an objectively reasonable perception that the father had apparent authority. These facts included the father's ownership of the house and payment of the utility bill that provided Internet service, the father's statement that he had unfettered access to his son's bedroom, and the computer's plain view location.[16]

The majority's holding was challenged in a strong dissent rejecting "the majority's implicit holding that law enforcement may use software deliberately designed to automatically bypass computer password protection based on third-party consent without the need to make a reasonable inquiry regarding the presence of password protection and the third party's access to that password." Acknowledging that the pervasive development of computer password technology presented a unique challenge to law enforcement, the dissent opined that such difficulty "does not and cannot negate Fourth Amendment protection to computer storage nor render an expectation of computer privacy unreasonable."[17]

Conclusion

Significant questions remain regarding the balance between personal privacy and security and law enforcement efforts, particularly in the realm of electronically stored information. While courts may seek to insure that criminals cannot use encryption techniques to defeat otherwise valid subpoenas and warrants, it seems reasonable to ask to what extent a citizen can be expected to cooperate in these efforts without waiving his own constitutional protections. In the era of cloud computing and detailed encryption and storage of computer files, these issues are likely to waft up to the Supreme Court.

1. See, e.g., Elkan Abramowitz and Barry A. Bohrer, "Search and Seizure of Digital Evidence: Evolving Standards," NYLJ (March 1, 2011); Abramowitz and Bohrer, "Further Developments on Privacy Rights in an Electronic Era," NYLJ (Jan. 5, 2010); Abramowitz and Bohrer, "Expansion of Border Searches to Laptops, Electronic Items," NYLJ (May 6, 2008).
2. __ F.3d__, 2012 WL 579433 (Feb. 23, 2012).
3. Id. at *2.
4. 96 S. Ct. 1569, 1581 (1976).
5. 120 S. Ct. 2037 (2000).
6. 2012 WL 579433, *7.
7. 2009 WL 424718 (D.Vt. Feb. 19, 2009).
8. Id. at *3 (citing *United States v. Doe*, 1 F.3d at 93). Originally, the grand jury subpoena to Boucher requested the production of the password used by Boucher to access the encrypted data. A magistrate judge found that the privilege against self-incrimination protects against compelling such a disclosure. 2007 WL 4246473 (D.Vt. Nov. 29, 2007). A United States District Court in the Eastern District of Michigan reached the same conclusion in *United States v. Kirschner* citing Supreme Court precedent finding "this type of procured testimony," considered by the government as the equivalent of providing a combination to a locked safe, to be protected by the Fifth Amendment. 2010 WL 1257355 (E.D.Mich. March 30, 2010).
9. __F. Supp.2d__, 2012 WL 182121 (D. Colo. Jan. 23, 2012).
10. 2012 WL 182121 at *4.
11. 2012 WL 579433 at *10 n. 27.
12. As an aside, the Court noted that the very fact that the government sought and the district court granted Doe limited immunity with respect to the production of the hard drive implied that the act itself was testimonial. Id. at *3 n. 13.
13. Id. at *11.
14. Id. at *12 (citing *Hubbell*, 120 S. Ct. at 2041-42).
15. 483 F.3d 711 (10th Cir. 2007), cert. denied, 128 S. Ct. 1738 (2008).
16. Id. at 720-21.
17. Id. at 722-23.