Federal Evidence Review

Highlighting Recent Federal Evidence Cases & Developments

Volume 9, Number 8 **www.FederalEvidence.com** **August 2012**

About The Federal Evidence Review

The Federal Evidence Review highlights recent federal evidence cases and developments. The Review is a monthly legal journal distributed via e-mail in a downloadable and searchable PDF with links to many of the covered published cases. Information on the Review is available online at: **www. FederalEvidence.com**

The Federal Evidence Review:

- Monitors current federal evidence developments, cases and trends
- Serves as a key reference source for practitioners at all litigation stages
- Identifies key evidence issues and ideas as they develop
- Tracks recent evidence developments and trends
- Maintains your advantage on evidence law by making it easier to use recent evidence cases in your practice

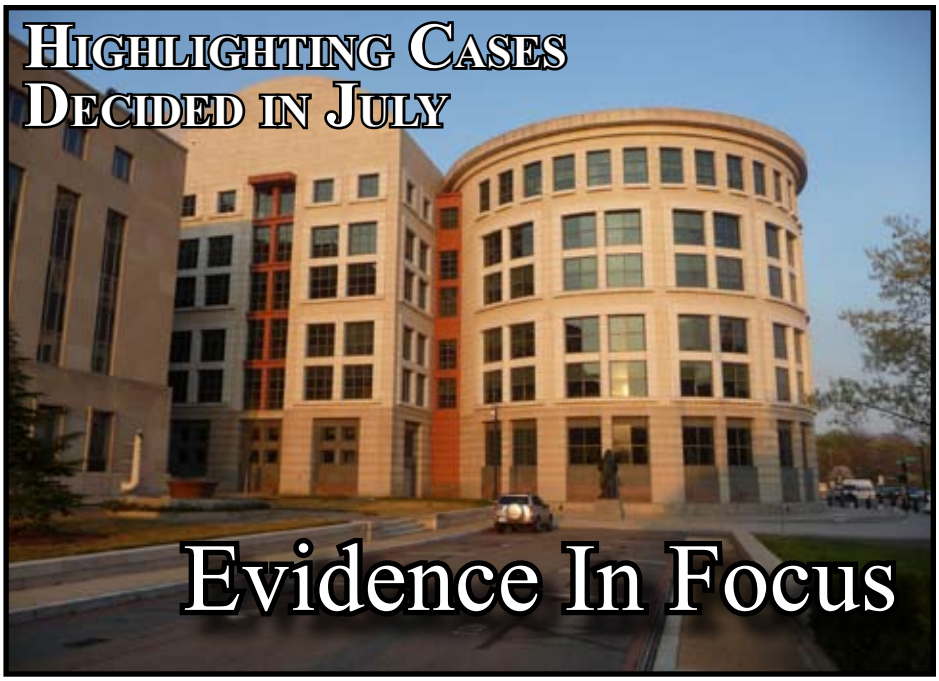
Federal Evidence Review Coverage

Cases Covered This Issue:

- Cases Covered: 38
- Evidence Principles: 96
- Cases Covered Since Vol. 1, No. 1 (August 2004): +2847

www.FederalEvidence.com

Subscription information available at: www.FederalEvidence.com



Evidence Viewpoints®: Compelling An Encrypted Password: As part of the *Evidence Viewpoints®* series, a federal prosecutor and defense attorney offer their perspectives on the extent that the government may compel an individual to provide a password to encrypted computer files under the Fifth Amendment; only a few published cases have addressed this issue (p. 800)

➢ *Recent Case Experience*: The authors were recently on opposing sides in the case of *In Re: Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335 (11th Cir. Feb. 23, 2012) (Nos. 11-12268, 11-15421), in which the Eleventh Circuit reversed an order compelling production of unencrypted computer contents after holding that the "decryption and production of the hard drives' contents would trigger Fifth Amendment protection because it would be testimonial, and that such protection would extend to the Government's use of the drives' contents"

Confrontation And Lab Report Certification, Notations And Chain Of Custody: Eighth Circuit concludes there was no Confrontation Clause error, and if so, no plain error, in the government's failure to call the lab supervisor and lab techni-

***Evidence In Focus* continued on next page ➔**

Decryption As Privileged Testimony Under The Fifth Amendment

Chet Kaufman

The exponential growth of technology in the computer age affects many societal interests, including national defense, personal privacy, standard business practices, corporate security, and crime prevention. While the digital age rapidly advances, its applicable law continues to emerge slowly and incrementally. New technology collided with the force of law in the recent decision of *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011 (United States v. John Doe)*, 670 F.3d 1335 (11th Cir. 2012). This case focused upon the Constitution's evidentiary limitation imposed on the Government when it seeks to force the target of a criminal investigation to decrypt encrypted data on the target's computer equipment.

In *Doe,* the target was suspected of engaging in the possession, creation, or production of child pornography. The Government obtained a warrant to search his hotel room and to seize and search his computer equipment, but its agents did not find any data they could read or understand. The drives or data appeared to have been encrypted. So, the Government tried to compel Doe to decrypt the data, over his invocation of the Fifth Amendment's privilege against compelled self-incrimination. The principal evidentiary and constitutional question in Doe's case was whether the privilege applied to the act of decryption.

I.
Encryption & Decryption

The basic purpose of encryption is to protect the confidentiality of information, ranging from trade secrets to sensitive personal information like credit card numbers, medical histories, or student records. It is especially useful for protecting information on small, portable devices like laptops, cell phones or USB drives, which can easily be stolen or lost.

Encryption is a process by which a person can change plain, understandable information into unreadable (or what the Court characterized as "nonsensical") letters, numbers and symbols using a mathematical algorithm. *Doe*, 670 F.3d at 1340. Only one who knows a special code – more commonly called an encryption key, password or passphrase – can decrypt or decipher the information to make it readable again. Efforts to defeat encryption often focus on trying to obtain the encryption key in some way.

Encryption is a useful tool for the Government and private sector alike. Computer and software manufacturers consider it basic security and include encryption tools as a standard feature on most new computers. For example, Microsoft's Windows comes with the Bitlocker Drive Encryption feature, while Apple's Mac OS X 10 operating system comes with FileVault. A brief web search shows that other encryption tools are available, including PGP ("Pretty Good Privacy"), and GNU Privacy Guard.

Some encryption tools, like the TrueCrypt application in Doe's case, are open source applications that can be

This *Evidence Viewpoints*® series presents articles by opposing counsel in *In Re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335 (11th Cir. 2012) [http://federalevidence.com/pdf/KeyCases/CTA/InreGJSubpoena-Doe.pdf] on page 801 and page 809 regarding some of the challenges in dealing with a government request for encrypted information on a computer.

Evidence Viewpoints® *is a periodic feature which highlights and explores significant and noteworthy evidence issues.*

downloaded from the internet at no charge to the end user. TrueCrypt provides the ability to encrypt individual data files, entire disks, or portions of disks (called volumes). If the entire hard drive is protected, the user must enter the encryption key every time the computer is turned on. Otherwise, the encryption key is needed to access protected data.

TrueCrypt is designed to make it difficult for an unauthorized person to know if particular data is actually encrypted. Without the encryption key, TrueCrypt-protected data appear as nonsensical letters, numbers and symbols. It is impossible for an unauthorized person to determine the presence, name, content, or amount of protected data. TrueCrypt also provides a feature called hidden volumes, which digitally subdivides encrypted disks or volumes with one or more extra layers of protection, requiring a separate and distinct encryption key to enter each hidden volume. TrueCrypt is designed so as to make it difficult for an unauthorized person to even know if hidden volumes exist. *See* http://www.truecrypt.org. TrueCrypt was found on Doe's laptop computer.

II. Traditional Search & Seizure In A Digital World

Law enforcement agents typically use their investigative warrant and subpoena authority to look for evidence. Often, this evidence is found in tangible form, such as photographs, correspondence, records related to communications, business and accounting. In computer searches, the presumption is that digital data, when legibly printed or otherwise displayed in traditional document form, would be admissible and/or would lead to other evidence admissible under the standard rules of evidence.

In Doe's case, the disk drives themselves had no evidentiary significance absent the Government's knowledge of their contents. They would be as worthless as a map of the Fountain of Youth with no identifiable markings on it. If the drives were to have any significance, the Government had to get them decrypted.

In effect, the Government's view was that the act of decryption was a negligible step in obtaining the tangible evidence it was otherwise constitutionally and legally authorized to examine and introduce against Doe. The only important factor, the Government argued, was that it lawfully possessed the computer equipment on which suspected encrypted contraband existed. After all, the Government had obtained a warrant to seize and search Doe's computer equipment. The Government thus asked the Eleventh Circuit to focus on its purported compliance with the Fourth Amendment.

By and large, practitioners principally look to the Fourth Amendment to regulate the authority of Government to gather tangible evidence. The Fourth Amendment authorizes the Government to search and seize "persons or *things*" so long as doing so is "reasonable." U.S. Const. amend. IV (emphasis supplied). The Fourth Amendment permits Government to use force or compulsion, too, provided it is reasonable. An unreasonable search and seizure unconstitutionally intrudes upon the "right of the people to be secure in their persons, houses, papers, and effects." *Id*.

Fifth Amendment Self-Incrimination Clause: U.S. Const. amend. IV.

"No person … shall be compelled in any criminal case to be a witness against himself…. "

In contrast, the Fifth Amendment's privilege against compelled self-incrimination does not permit the Government to use force or compulsion to extort testimonial evidence. It does not permit the Government to compel testimony even if doing so may be considered reasonable by some objective measure. Its focus is not on the surrender of "things." Its focus is on thought lodged in the mind of the witness.

The Fifth Amendment privilege applies to "a Testimonial Communication that is incriminating." *Fisher v. United States*, 425 U.S. 391, 408 (1976). The Constitution's framers feared, with much historical support, "that self-incriminating statements will be elicited by inhumane treatment and abuses." Such compulsion would violate our American "sense of fair play" and our respect for the individual, innocent or guilty. They feared that allowing compelled self-incrimination could lead to an "inquisitorial system of criminal justice," which the Framers rejected. *Murphy v. Waterfront Com'n of New York Harbor,* 378 U.S. 52, 55 (1964).

III. Testimonial Status Of Production/ Decryption Depends On Government Knowledge

The Fifth Amendment privilege against compelled self-incrimination has at its core three elements: "(1) compulsion, (2) a testimonial communication or act, and (3) incrimination." *Doe*, 670 F.3d at 1340. Compulsion and incrimination were undisputed, so the issue in Doe's case focused on the second element.

In effect, the Government argued that digital evidence in the form of encrypted data is tangible evidence, and the Government's authority to access decrypted files should be treated no differently under the Fifth Amendment than the Government's authority to access tangible evidence is treated under the Fourth Amendment. Doe argued that the Fourth Amendment does not apply because compelled decryption is a testimonial act under the Fifth Amendment. Doe argued that exposing the contents of one's mind, by, for example, revealing from memory the combination to a safe, is a testimonial act, whereas exposing one's physical characteristics, like in a blood sample or a handwriting exemplar, is not. *United States v. Hubbell,* 530 U.S. 27, 34-35, 43 (2000) (explaining the distinction, using as an example of a testimonial act revealing "the combination to a wall safe," and holding that Hubbell's act of revealing the existence and location of 13,120 pages of documents was a testimonial act); *see also United States v. Ponds*, 454 F.3d 313, 325-27 (D.C. Cir. 2006) (revealing the existence, identity, or location of many documents was a testimonial act); *cf. United States v. Green*, 272 F.3d 748, 751 (5th Cir. 2001) (finding Fifth Amendment violated when agents had Green open two combination locks and direct officers to those locked containers after he invoked his right to counsel in a custodial interrogation). The Eleventh Circuit agreed with Doe that the crux of the dispute was whether the act of decryption was a testimonial act within the meaning of the Fifth Amendment.

Noteworthy Trial & Appellate Cases Cited

• *United States v. Green*, 272 F.3d 748, 753 (5th Cir. 2001) [http://federalevidence.com/pdf/2006/07A-July/US.v.Ponds.pdf]("[O]pening the combination locks ... were testimonial and communicative in nature" under the Fifth Amendment)

• *United States v. Kirschner,* 823 F.Supp.2d 665, 669 (E.D. Mich. Mar. 20, 2010) [http://federalevidence.com/pdf/2006/07A-July/US.v.Ponds.pdf]("This case is not about producing specific documents - it is about producing specific testimony asserting a fact.")

• *United States v. Ponds*, 454 F.3d 313, 320 (D.C. Cir. 2006) [http://federalevidence.com/pdf/2006/07A-July/US.v.Ponds.pdf] ("[T]he applicability of the Fifth Amendment turns on the level of the government's prior knowledge of the existence and location of the produced documents.")

The Government, arguably, made answering that question pretty simple. "If the decryption of the hard drives would not constitute testimony, one must ask, 'Why did the Government seek, and the district court grant, immunity for Doe's decryption?' The answer is obvious: Doe's decryption would be testimonial." *Doe*, 670 F.3d at 1341. *Cf. Hubbell*, 530 U.S. at 43-44 (noting a similar arguable concession by the Government in Hubbell's district court proceedings).

Nonetheless, the Eleventh Circuit put little weight on the Government's conduct. Instead, it analyzed the issue in light of *Fisher* and *Hubbell.* Together, those decisions held in relevant part that if a witness invokes the privilege and is nonetheless compelled by subpoena to do an act

that communicates a fact – a testimonial act – that is self-incriminating or leads to incriminating evidence, such evidence is inadmissible unless the Government can independently prove the incriminating fact, or there is an appropriate grant of immunity.

So, the first question the Court had to answer was what facts, if any, would be communicated by the act of production/decryption. The Eleventh Circuit agreed with Doe that decryption "would be tantamount to testimony by Doe of his knowledge of the existence and location of potentially incriminating files; of his possession, control, and access to the encrypted portions of the drives; and of his capability to decrypt the files." *Doe,* 670 F.3d at 1346.

The second question the Court had to resolve was whether the Government could prove any of those facts without Doe's compelled act of production/decryption. The answer depended on what was already within the Government's knowledge.

Fifth Amendment protection does not extend to evidence the Government already possesses; it extends only to evidence the Government must acquire by compelling testimony. Had the Government – without aid of decryption – already known with "reasonable particularity" what contraband (if any) was on Doe's drives, *id*. at 1344 n.20, the act of decryption would have added nothing new and substantive to the Government's case.

In other words, proving its case to a petit jury would have been a "foregone conclusion," *id*. at 1343-44, if, without Doe's testimonial act of decryption, it could prove the existence and illegal nature of contraband as well as Doe's access, knowledge, possession, and control of it. "If … the Government could prove that it had knowledge of the files encrypted on Doe's hard drives, that Doe possessed the files, and that they were authentic, it could compel Doe to produce the contents of the files even though it had no independent source from which it could obtain the files." *Doe*, 670 F.3d at 1343 n.19.

The Eleventh Circuit held that the record did not support the Government, for all the Government knew was that the laptop contained "nonsensical characters and numbers." *Doe*, 670 F.3d at 1340. It could not prove that any data, no less any contraband, was secreted on any of Doe's computer equipment. The act of production/decryption would communicate facts not known to the Government. Therefore, the "foregone conclusion" doctrine could not be applied to circumvent the privilege. Only a proper grant of immunity could do that.

IV.
The Fifth Amendment & Production/ Decryption As Evidence Of Authentication

The Government agreed it had not offered Doe derivative use immunity, but said it did not matter. It took the position that it was enough to immunize Doe from using his act of production/decryption of the encrypted drives as evidence of authentication. Under that limited grant, the Government agreed it would not tell petit jurors how it came into possession of the decrypted documents, but it would still introduce the documents as substantive evidence against Doe. Thus, the third question the Eleventh Circuit had to resolve was whether immunizing Doe from using his act of production/decryption as evidence of authentication was sufficient to overcome the privilege. The Eleventh Circuit held it was not.

It has been long settled that the privilege against compelled self-incrimination may be overcome by a grant of immunity. 18 U.S.C. §§ 6002, 6003; *Kastigar v. United States,* 406 U.S. 441 (1972). The privilege protects a witness from the use and derivative use of any information obtained in violation of the privilege. *Doe*, 670 F.3d at 1349-52; *Kastigar*, 406 U.S. at 453-58. The Eleventh Circuit relied on the use and derivative use analysis as the Supreme Court did in *Hubbell*, and the District of Columbia Circuit did in *United States v. Ponds*, 454 F.3d 313 (D.C. Cir. 2006). Each of those decisions applied the rule that "[u]se and derivative-use immunity establishes the critical threshold to overcome an individual's invocation of the Fifth Amendment privilege against self-incrimination. No more protection is necessary; no less protection is sufficient." *Doe,* 670 F.3d at 1351.

If Doe had the immunity Congress and the Constitution authorized, neither the act of production/decryption, the decrypted documents, nor other evidence obtained in reliance thereon, could be introduced against him. "[T]he Government cannot obtain immunity only for the act of production and then seek to introduce the contents

of the production, regardless of whether those contents are characterized as nontestimonial evidence, because doing so would allow the use of evidence derived from the original testimonial statement." *Doe,* 670 F.3d at 1351-52.

Despite that rule, the Government claimed Doe's immunity from use of the evidence as proof of authentication was sufficient here. It contended that proof Doe knew the existence of the contents, was responsible for creating, producing, or encrypting them, or had the ability to conceal them, were mere aspects of authentication. Any of these could assist the Government in establishing that the decrypted data "is what its proponent claims." FED. R. EVID. 901.

The Eleventh Circuit's opinion rejected that argument without elaboration, but it is worth some discussion here. The term "authentication" as used in this context was discussed in *Fisher*, where the Court tried to determine whether compelling a taxpayer to turn over papers prepared for him by his accountant might have some testimonial, self-incriminating significance as proof of authentication. The *Fisher* analysis equated authentication with "genuineness," nothing more. *Fisher,* 425 U.S. at 412-13 & n.14. *See also Doe v. United States,* 487 U.S. 201, 215-16 (1988) (discussing "existence," "control," "locat[ion]," "authentication," and "consent" as facts that may be derived from a testimonial act of production); *Hubbell*, 530 U.S. at 40-41 (discussing "existence," "authenticity," and "custody"). That accords with federal law. *See* FED. R. EVID. 901(a) ("The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims"). *See generally* BLACK'S LAW DICTIONARY 142 (8th ed. 2004) (authentication is "the act of proving that something (as a document) is true or genuine, esp. so that it may be admitted as evidence").

Moreover, the Supreme Court repeatedly has considered authentication as distinct from other testimonial aspects of the act of production. *See Hubbell,* 530 U.S. at 40-41 (discussing "existence," "authenticity," and "custody"); *Fisher*, 425 U.S. at 411-13 (discussing "existence," "location," "access," "possession," "control," and "authentication"); *Doe*, 487 U.S. at 215-16 (discussing "existence," "control," "locat[ion]," "authentication," and "consent").

Authoritative academic treatises also construe authentication more narrowly than did the Government. For instance, Professor Wigmore's treatise says authentication is "proving [a document's] genuineness or execution," WIGMORE ON EVIDENCE § 2128 (Chadbourne Rev. & 1991 Supp.), and is distinct from substantive factual issues such as proof of use or ownership, *id*. § 2129-30. MCCORMICK ON EVIDENCE VOL. 2 § 221 (6th ed. & 2010 Supp.), suggests the "principle justification" for the authentication of documents is "judicial skepticism," and the rule was created to constitute[] a necessary check on the perpetration of fraud." Authentication as a predicate for admissibility has been applied to electronic and computer-generated data as well as documents. *Id.* § 227.

The Government's proposed broad view of authentication cannot bear the weight of all this authority. Authentication is a simple concept that amounts to nothing more than proof that a piece of evidence is genuine. Proving the chain of custody of the drives would prove the drives were genuine. Proving that the decrypted documents came from Doe's computer would prove they were genuine. But that is not what concerned Doe or the Eleventh Circuit. The Court knew that Doe's decryption would also be proof that Doe knew the contents of his laptop, that he possessed and controlled them, that he encrypted them, and that he could decrypt them. By offering not to introduce his decryption as proof of authentication (genuineness), while nonetheless introducing the decrypted documents as substantive evidence, the Government was conceding nothing, making a hollow, meaningless promise. *Cf. Fisher,* 425 U.S. at 413 (noting that because the Government knew the subject documents were created by Fisher's accountants and not Fisher himself, Fisher "would be no more competent to authenticate the accountant's workpapers or reports by producing them than he would be to authenticate them if testifying orally.") (footnote omitted).

V.
What Does *Doe* Portend For The Future?

One insight that can be inferred from this decision is the rejection of the Government's claim that its interest in prosecuting criminals and producing the "truth," and/or its compliance with the Fourth Amendment, should trump the Fifth Amendment's protection against

inquisitorial justice and its distinction between tangible and testimonial evidence. The Government argued that failing to allow it to use the fruits of compelled decryption amounts to a concession to white collar criminals, gang members, hackers, and child pornographers that encrypting all inculpatory digital evidence will defeat the efforts of law enforcement officers. The court would thus sanction an individual's ability to deprive the justice system of evidence it needs to search for the truth, regardless of probable cause (which was found in issuing a warrant for seizure of Doe's computer equipment), life-or-death, emergencies, or any other consideration. This, the Government argued, would be an unprecedented and a dangerous absolute limitation.

The Government's parade of horribles was cast aside by the Eleventh Circuit in its observation that "the privilege against self-incrimination carves out a significant exception to the Government's ability to obtain every man's evidence." *Doe*, 670 F.3d at 1341. No reasonable person would challenge the legitimacy of Government interests in protecting individuals from crime and in prosecuting wrongdoers. The framers were well aware of those interests. But they balanced the interests in favor of the privilege because of "our realization that the privilege, while sometimes 'a shelter to the guilty,' is often 'a protection to the innocent.'" *Murphy v. Waterfront Com'n of New York Harbor,* 378 U.S. 52, 55 (1964) (quoting *Quinn v. United State*s, 349 U.S. 155, 162 (1955)).

If in a future case the Government has knowledge about the contents of a decrypted computer drive, it might be able to pass the "foregone conclusion" test and achieve a different result. On the other hand, if it is just another fishing expedition, as in *Hubbell* and *Doe*, there is no reason to think the Government will be permitted to compel decryption.

Despite the groundbreaking nature of *Doe*, it is questionable that the decision is bound to have a wide impact. Even if there is proof of "(1) compulsion, (2) a testimonial communication or act, and (3) incrimination," *Doe,* 670 F.3d at 1341, there exists another factor, akin to standing, which the Eleventh Circuit had no need to discuss but which may be of special importance as we look to future applications of the privilege in the digital world.

As rooted as the privilege may be, it applies only to natural persons, including resident aliens. *United States v. Balsys,* 524 U.S. 666, 671 (1998). For more than a century, the Supreme Court has perpetuated a collective entity doctrine which provides that "the privilege could not be employed by an individual to avoid production of the records of an organization, which he holds in a representative capacity as custodian on behalf of the group." *United States v. White,* 322 U.S. 694, 699-700 (1944) (holding unincorporated labor union has no privilege); *see also*, *e.g.*, *Wilson v. United States,* 221 U.S. 361, 384-85 (1911) (corporations); *United States v. Fleischman,* 339 U.S. 349, 357-58 (1950) (Joint Anti-Fascist Refugee Committee); *Rogers v. United States,* 340 U.S. 367, 371-72 (1951) (Communist Party of Denver); *McPhaul v. United States,* 364 U.S. 372, 380 (1960) (Civil Rights Congress); *Bellis v. United State*s, 417 U.S. 85, 88 (1974) (partnerships); *Braswell v. United States*, 487 U.S. 99, 107 (1988) (corporation president could not interpose Fifth Amendment objection to compel production of corporate records, even if act of production might prove personally incriminating).

The collective entity doctrine may also be fairly characterized as the white-collar crime exception to the privilege. As the Supreme Court stated, "recognizing a Fifth Amendment privilege on behalf of the records custodians of collective entities would have a detrimental impact on the Government's efforts to prosecute 'white-collar crime,' one of the most serious problems confronting law enforcement authorities. 'The greater portion of evidence of wrongdoing by an organization or its representatives is usually found in the official records and documents of that organization. Were the cloak of the privilege to be thrown around these impersonal records and documents, effective enforcement of many federal and state laws would be impossible.'" *Braswell,* 487 U.S. at 115 (quoting *White,* 322 U.S. at 700).

Because of the collective entity doctrine, the essential holding in *Doe,* finding decryption to be a testimonial act, may as a practical matter have a limited reach. As of this writing, no reported appellate decisions have ventured into that arena, no such pending litigation has come to this author's attention, and no academic literature appears to have addressed that question.

There is still one other potential limitation on the reach of *Doe* worth mentioning — escrowing. In 1998, Congress

entertained controversial suggestions in the hopes of avoiding the testimonial act-of-production problem with encryption. This included a requirement that those who make or use encryption technologies turn over their digital keys to third parties in order to preserve ready access by Government to the encrypted information. *See Privacy In The Digital Age: Encryption And Mandatory Access*, 1998: HEARINGS BEFORE THE SUBCOMMITTEE ON THE CONSTITUTION OF THE SENATE COMMITTEE ON THE JUDICIARY, 105th Congress (1998) (at page 45) (statement of Kathleen M. Sullivan, Professor, Stanford Law School)) (*available at* http://federalevidence.com/pdf/Comput/USCong.Sen.J.105-87.pdf).

A close cousin of escrowing reared its head in the last year or two when the executive branch said it wanted regulations to require communication services to be prepared to decrypt messages if ordered to do so. *See* Charlie Savage, *U.S. Tries to Make It Easier to Wiretap the Internet*, NEW YORK TIMES Sept. 27, 2010 (*available at* https://www.nytimes.com/2010/09/27/us/27wiretap.html) (last accessed Aug. 26, 2012); Declan McCullagh, *FBI: We're not demanding encryption back doors*, CNET NEWS, February 17, 2011 (*available at* http://news.cnet.com/8301-31921_3-20032910-281.html) (last accessed Aug. 26, 2012). This is a subject worthy of treatment too nuanced to discuss here. *See, e.g.,* Adam C. Bonin, *Protecting Protection: First and Fifth Amendment Challenges to Cryptography Regulation*, 1996 U. CHI LEGAL F. 495 (1996); D. Forest Wolfe, *The Government's Right to Read: Maintaining State Access to Digital Data in the Age of Impenetrable Encryption*, EMORY L.J. 711 (2000).

Moreover, current law provides some practical means by which the Government can avoid the Fifth Amendment decryption problem. Investigators can install a keystroke monitor on suspected hardware to obtain the encryption keys, or seize a computer while operating with the files already decrypted. Of course, both of these options presuppose adherence to the Fourth Amendment.

VI.
Doe Broke New Ground But Leaves Much To Be Decided

Only a few district courts have touched the question of encryption. To date, no state courts of last resort have done so. *Doe* broke new ground by finding a limited grant of act of production immunity was insufficient to overcome the privilege against compelled self-incrimination. These holdings imposed new limits on the Government's use of the grand jury subpoena as an investigative tool. As a practical matter, however, *Doe* may end up having limited reach because of limitations on the privilege and the availability of other investigative tools the Government may be able to employ.

Author: As an Assistant Federal Public Defender in the Northern District of Florida, Chet Kaufman was lead defense counsel in *In re Grand Jury Subpoena Duces Tecum* Dated March 25, 2011 (*United States v. John Doe*), 670 F.3d 1335 (11th Cir. 2012). He is an appellate specialist, board certified by The Florida Bar in criminal appeals. He has worked in the federal system for more than ten years. Previously he worked for seven years arguing capital cases for the Public Defender of the Second Judicial Circuit, State of Florida. He clerked for four years at the Supreme Court of Florida for Rosemary Barkett, then-Justice and-Chief Justice, and now a Judge on the Eleventh Circuit. He graduated with high honors from the Florida State University College of Law, where he was executive editor of the Law Review. He was a newspaper reporter before attending law school.
Mr. Kaufman extends his thanks to Marcia Hofmann and Hanni Fakhoury of the Electronic Frontier Foundation for EFF's participation as an amicus in In re Grand Jury and as well as in the preparation of this article.

United States Supreme Court
Selected Fifth Amendment Self-Incrimination Cases

• *Baltimore City Dept. of Social Services v. Bouknight,* 493 U.S. 549, 555 (1990) [http://federal-evidence.com/node/1547]("The possibility that a production order will compel testimonial assertions that may prove incriminating does not, in all contexts, justify invoking the privilege to resist production.")

• *Braswell v. United States*, 487 U.S. 99, 117 (1988) [http://federalevidence.com/pdf/KeyCases/Braswell.v.US.pdf] ("Although a corporate custodian is not entitled to resist a subpoena on the ground that his act of production will be personally incriminating, we do think certain consequences flow from the fact that the custodian's act of production is one in his representative [of corporation] rather than personal capacity.")

• *United States v. Balsys*, 524 U.S 666, 671 (1998) [http://federalevidence.com/node/1547](In this case there is no basis for concluding that the privilege will lose its meaning without a rule precluding compelled testimony when there is a real and substantial risk that such testimony will be used in a criminal prosecution abroad.)

• *Doe v. United States*, 487 U.S. 201, 215-16 (1988) [http://federalevidence.com/pdf/KeyCases/Doe.Official.pdf] (Completion of a consent directive was not testimonial under the Fifth Amendment "because neither the form, nor its execution, communicates any factual assertions, implicit or explicit, or conveys any information" to the Government.)

• *Fisher v . United States,* 425 U.S. 391, 411 (1976) [http://federalevidence.com/pdf/KeyCases/Fisher.pdf]("The existence and location of the papers are a foregone conclusion and the taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers. Under these circumstances by enforcement of the summons 'no constitutional rights are touched. The question is not of testimony but of surrender.'" (quoting *In re Harris*, 221 U. S. 274, 279 (1911))

• *United States v. Hubbell*, 530 U.S. 27, 34-35, 43 (2000) [http://federalevidence.com/pdf/2000/US_v._Hubbell.pdf] (The act of production of records compelled by a subpoena "had a testimonial aspect, at least with respect to the existence and location of the documents" which implicated the Fifth Amendment and "could not be compelled … without first receiving a grant of immunity....")

• *Kastigar v. United States*, 406 U.S. 441, 453 (1972) [http://federalevidence.com/pdf/KeyCases/Kastigar.pdf] ("We hold that such immunity from use and derivative use is coextensive with the scope of the privilege against self-incrimination, and therefore is sufficient to compel testimony over a claim of the privilege.")

• *Murphy v. Waterfront Com'n of New York Harbor*, 378 U.S. 52, 55 (1964) [http://federalevidence.com/node/1546] ("[A] ... witness may not be compelled to give testimony which may be incriminating under federal law unless the compelled testimony and its fruits cannot be used in any manner by federal officials in connection with a criminal prosecution against him.")