



# 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](http://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

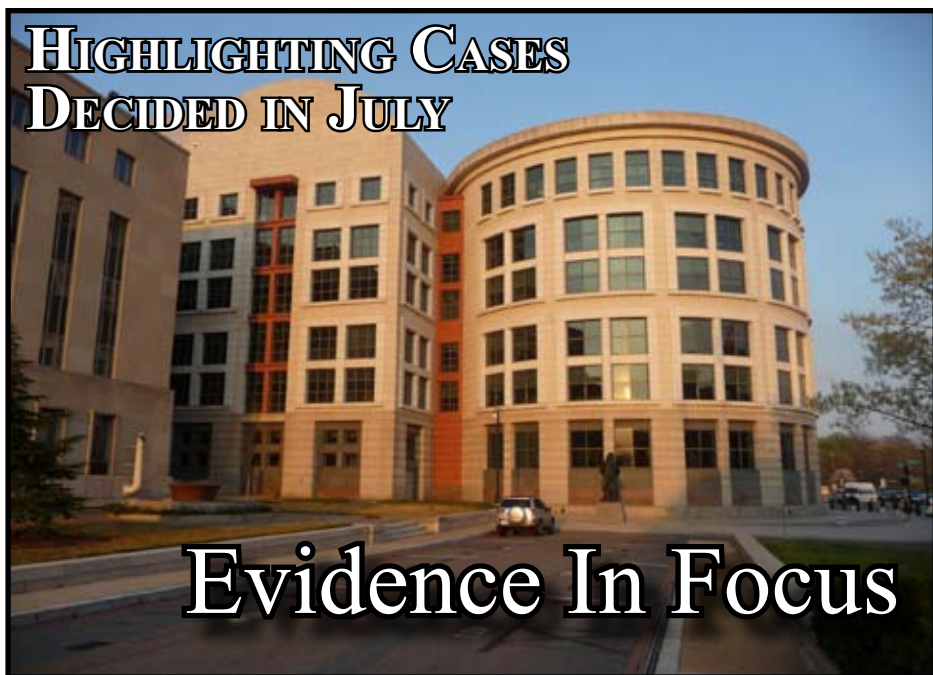
## FEDERAL EVIDENCE REVIEW Coverage

### Cases Covered This Issue:

- Cases Covered: 38
  - Evidence Principles: 96
  - Cases Covered Since Vol. 1, No. 1 (August 2004): +2847
- [www.FederalEvidence.com](http://www.FederalEvidence.com)

Subscription information available at: [www.FederalEvidence.com](http://www.FederalEvidence.com)

## HIGHLIGHTING CASES DECIDED IN JULY



# Evidence In Focus

**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”

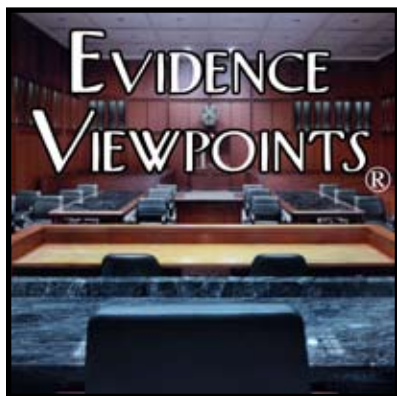
**Confrontation And Lab Report Certification, Notations And Chain Of Custody:** Eighth Circuit concludes there was no Confrontation Clause error, and if so, no plain error, in the government’s failure to call the lab supervisor and lab techni-

*Evidence In Focus* continued on next page →

**Evidence Case Docket:** Evidence issues organized by FRE (p. 815)  
**Table Of Contents** (p. 791)  
**Circuits At A Glance:** Summary of evidence cases by circuit (p. 897)  
**Pending Amendments To The Federal Rules Of Evidence** (p. 928)  
**Using The Federal Evidence Review** (p. 813)

# Decoding Encryption for Litigators

*James Silver*



**E**ncryption is the alteration of information so that only people with special knowledge can understand it. In one form or another, encryption has been around for a long time: Julius Caesar used a cipher to alter his battlefield

communications; Thomas Jefferson's wheel cipher device is on display at Monticello. Modern encryption technology uses mathematics and computers to allow users to encrypt large amounts of data quickly, and it is increasingly automatic and invisible to the user.

Like most technologies, encryption can be used for purposes both good and bad. It can thwart identity thieves or the agents of tyrannical governments; but it can also protect child-pornography collections or terrorist plots. For civil and criminal litigants, and the justice system in general, the rise of digital encryption poses a distinct problem: the unavailability, or indecipherability of encrypted evidence.

If a case turns on the contents of a laptop, what can be done if the laptop is completely encrypted? As more information is stored digitally, and more digital information encrypted by default, the problem becomes more complicated. Increasing amounts of evidence are encrypted. Furthermore, even free-of-charge encryption software can thwart high-powered, court-authorized efforts to defeat it.

This article offers a brief primer on encryption, summarizes relevant federal legal principles, suggests methods to obtain encrypted evidence, and concludes by noting the rise of biometric-based encryption and its implications.

## I. Encryption: A Short Primer For Litigators

Ancient encryption relied on secret ciphers and ingenious mechanical devices. Modern encryption is a creature of applied mathematics. Cryptographers write encryption algorithms: mathematical functions that, when applied to unencrypted plaintext, transform it to encrypted ciphertext.

The best known algorithms are public, and have survived scrutiny by the cryptographic community. Despite being publicly available, these algorithms can keep plaintext secure when used with keys. Keys are specific values, usually kept private, that may be short or complex passwords chosen by users, values derived from biometric analysis (*e.g.*, fingerprint or retina scans), computer files such as images or music, or some combination thereof. Encryption usually works best when it employs one of the public, peer-reviewed algorithms with a sufficiently-complex key that is hard to guess and kept secret. Sometimes the same key is used for both encryption and decryption; sometimes not.

This *Evidence Viewpoints*® series presents article 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.

Copyright © 2012 FederalEvidence.com  
All Rights Reserved

Encryption is increasingly built into operating systems and computer hardware. Formidable encryption can be downloaded free-of-charge. Hardware manufacturers already sell self-encrypting hard drives and thumb drives, self-protecting devices whose contents are encrypted by default. When these devices are powered down, or even suddenly unplugged, they immediately encrypt.

Encryption can be used to protect both data at rest, and data in motion. If you have ever logged into your bank or brokerage account online, you have probably used encryption to protect your communications with the bank, perhaps without knowing it. We should expect that, even as encryption becomes more prevalent, it will become less visible to users and more automatic. For example, instead of struggling to remember a password to log-on to our computers, our computers may soon recognize our voices, retinas, faces,<sup>1</sup> or other unique features, instead of passwords. This technology is already available. The legal significance of this likely increase in the use of biometric and other non-password authentication is discussed below.

Finally, encryption is different from password protection. Not every password prompt has encryption behind it; conversely, not all encryption requires passwords — encryption can also work with computer files, fingerprints, or other authenticating data. A qualified computer forensic examiner may be able to view information that is password-protected but not encrypted.

### Federal Evidence Blog Series regarding "Compelling Access To Encrypted Information:"

• **Part I** - *In re Boucher*, 2009 WL 424718 (D. Vt. Feb. 19, 2009) (government observed child pornography on defendant's laptop during border search before laptop re-encrypted) [ <http://federalevide.com/pdf/2007/11-November/InreBoucher.pdf> ] **blog:** <http://federalevide.com/node/368> ]

• **Part II** - *United States v. Fricosu*, 841 F.Supp.2d 1232 (D. Colo. Jan. 23, 2012) (defendant discussed contents of encrypted laptop in conversation recorded by government) [ <http://federalevide.com/pdf/Comput/Fricosu.Ord.1-23-12.pdf> ] **blog:** <http://federalevide.com/node/1393> ]

• **Part III** - *In Re: Grand Jury Subpoena Duces Tecum Dated March 25, 2011 (Doe v. United States)*, 670 F.3d 1335 (11th Cir. Feb. 23, 2012) (reversing order compelling production of unencrypted computer contents since the "decryption and production of the hard drives' contents would trigger Fifth Amendment protection" because it would be testimonial) [ <http://federalevide.com/pdf/KeyCases/CTA/InreGJSubpoena-Doe.pdf> ] **blog:** <http://federalevide.com/node/1415> ]

• **Part IV** - *United States v. Hatfield*, 2010 WL 1423103 (E.D.N.Y. Apr. 7, 2010) (enforcing court order to produce metadata over Fifth Amendment privilege because, *inter alia*, defendant's possession of metadata was foregone conclusion) [ <http://federalevide.com/pdf/2012/08Aug/US.v.Hatfield.pdf> ] **blog:** <http://federalevide.com/node/1533> ]

• **Part V** - *United States v. Gavegnano*, 305 Fed. Appx. 954 (4th Cir. 2009) (any testimonial aspect of defendant's providing password was foregone conclusion since government independently proved he was sole user of computer) [ <http://federalevide.com/pdf/Comput/U.S.%20v.%20Gavegnano.pdf> ] **blog:** <http://federalevide.com/node/1545> ]

<sup>1</sup>To an extent, this future is already here: mobile devices running the latest version of the Android operating system may be unlocked via facial recognition. However, this unlocking differs from decryption, and this difference is discussed below.

## II. Federal Legal Principles

Federal law has an increasing amount to say about when the decryption of digital media may be compelled. We begin with the Constitution. The Self-Incrimination Clause of the Fifth Amendment provides that “No person . . . shall be compelled in any criminal case to be a witness against himself . . .” This well-known language raises a bulwark against traditions of inquisition and torture that the Framers wisely sought to end.<sup>2</sup>

The Supreme Court has explained that “the word ‘witness’ in the constitutional text limits the relevant category of compelled incriminating communications to those that are ‘testimonial’ in character.” *United States v. Hubbell*, 530 U.S. 27, 34 (2000). Thus, the privilege “applies only when the accused is compelled to make a testimonial communication that is incriminating.” *Baltimore City Dept. of Social Services v. Bouknight*, 493 U.S. 549, 554 (1990). The privilege can be invoked in civil proceedings, although a fact-finder may draw an adverse inference from a party’s invocation. *Baxter v. Palmigiano*, 425 U.S. 308, 316-19 (1976). It is for courts to determine whether a particular communication would be incriminating. *Rogers v. United States*, 340 U.S. 367, 375 (1951).

Certain acts, though incriminating, are not within the privilege against self-incrimination, because they are not communications. *Doe v. United States*, 487 U.S. 201, 211 (1988). This includes many acts that invade privacy or that could provide considerable incriminating information, such as furnishing a blood, handwriting, or voice sample; standing in a lineup; wearing particular clothing, *id.* (citing cases); and producing a child in response to a court order, *see Bouknight*, 493 U.S. at 559; *Hubbell*, 530 U.S. at 35.

The act of producing evidence may communicate information, and therefore be testimonial. An example of this is where a defendant “tacitly conced[es] the existence of the [evidence] and [its] possession or control,” as well as conveys the “belief that the papers are those described in the subpoena.” *Fisher v. United States*, 425 U.S. 391,

410 (1976). However, the act of producing evidence does not have testimonial significance if the seeking party already knows that the evidence exists and that the defendant must possess and control it. In *Fisher*, the Supreme Court wrote that “[i]t is doubtful that implicitly admitting the existence and possession of . . . papers rises to the level of testimony” because “[t]he existence and location of the papers are a foregone conclusion and the [defendant] adds little or nothing to the sum total of the Government’s information by conceding that he in fact has the papers.” *Id.* at 411. Here, the act of production was not testimony, but mere surrender.

This “foregone-conclusion rationale,” as subsequent courts have called it, is the most viable legal justification for compelling decryption. Four courts have approved the compelled decryption of digital media because the Government already knew enough about the encrypted matters to render any testimonial aspects of the decryption a foregone conclusion. *United States v. Gavegnano*, 305 Fed. Appx. 954 (4th Cir. 2009) (any testimonial aspect of defendant’s providing password was foregone conclusion since Government independently proved he was sole user of computer); *United States v. Fricosu*, 841 F.Supp.2d 1232 (D. Colo. Jan. 23, 2012) (defendant discussed contents of encrypted laptop in conversation recorded by Government); *United States v. Hatfield*, 2010 WL 1423103 (E.D.N.Y. Apr. 7, 2010) (enforcing court order to produce metadata over Fifth Amendment privilege because, *inter alia*, defendant’s possession of metadata was foregone conclusion); *In re Boucher*, 2009 WL 424718 (D. Vt. Feb. 19, 2009) (Government observed child pornography on defendant’s laptop during border search before laptop re-encrypted).

However, most recently, the Eleventh Circuit held that the Government did not know enough about certain encrypted digital media in order to satisfy the foregone-conclusion rationale, but approved of the *Fricosu* court’s ruling because defendant had already “essentially admitted every testimonial communication that may have been implicit in the production of the unencrypted contents.” *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011 (“John Doe”)*, 670 F.3d 1335, 1349 n.27 (11th Cir. 2012).

<sup>2</sup>Leonard W. Levy, ORIGINS OF THE FIFTH AMENDMENT 3 (1999). This book thoroughly examines the history behind the Fifth Amendment.

The *Doe* court reached this result even though the Government had obtained a search warrant for the encrypted media. The court set out a test for the satisfaction of the foregone-conclusion rationale: a party must show with some reasonable particularity that [it] seeks a certain file and is aware, based on other information, that (1) the file exists in some specified location, (2) the file is possessed by the target of the subpoena, and (3) the file is authentic. *Id.* While it is somewhat unclear what the court meant by “authentic,” parties can cite the *Doe* court’s approval of *Fricosu* to argue that it is not necessary to have actually observed the encrypted files to meet this standard.

Although the *Doe* court recognized the “settled proposition” that a person may be required to produce specific documents even if they are incriminating, because their creation was not compelled, *id.* at 1342, citing *Hubbell*, 530 U.S. at 35-36, the court decided that the case turned instead on whether *Doe*’s production of the documents would have sufficient testimonial quality to trigger Fifth Amendment protection. The court concluded that *Doe*’s act of decryption and production would have been testimonial, and that the Government could not compel *Doe* to decrypt the media without granting use immunity as to the media’s contents. *Id.* at 1349-52.

### III.

## Suggestions For Obtaining Encrypted Evidence

Based on these general federal legal principles, several considerations can be useful in the effort to obtain encrypted evidence:

### ***A. Encryption Can Be Hard To Detect In The First Place***

Encryption providers are in the business of protecting their users’ data from searching adversaries. What better way to do this than by not only encrypting the data, but concealing the presence of the encryption itself? If you have reason to believe that some evidence in your case may be encrypted (and if your case involves digital evidence, you increasingly do), then don’t expect the encryption to be readily-visible. You may need help finding it, which leads to the next suggestion.

### ***B. Hire A Qualified Computer Forensic Examiner***

Computer forensics is the collection and analysis of data from computers and related devices in order to admit the data in court. As computer forensics is a young discipline, it can be difficult to determine who is qualified. For starters, consider examiners trained by the organizations listed in the box below. Your examiner should be able to distinguish between encryption and mere password-protection, and may attempt cryptographic techniques such as “brute force” attacks, in which multiple keys are tried against the encryption. A “dictionary attack” is a type of brute-force attack that works from a “dictionary” of likely keys.

#### **Computer Forensic Examiner Training Organizations**

*(Not listed in any particular order)*

- Guidance Software (<http://guidancesoftware.com>)
- Access Data (<http://accessdata.com>)
- ProDiscover (<http://prodiscover.com>)
- X-Ways (<http://x-ways.net>)
- SANS Institute (<http://computer-forensics.sans.org>)
- ISFCE (<http://isfce.com>)
- ECouncil (<http://eccouncil.org>)
- IACIS (<https://iacis.com>)

### ***C. Exhaustively Investigate The Encrypted Records***

It is important to exhaustively investigate the encrypted records and their users’ interactions with them. This goes to your ability to invoke the “foregone-conclusion” rationale.” Four key questions include:

- *What exactly is encrypted?*
- *Where are the encrypted files, both in terms of physical location in the world, and logical location on a particular device?*
- *Who is able to decrypt the files?*
- *How do you know this?*

Answer these questions, and you may be able to persuade a court to compel decryption.

#### ***D. Questions Witnesses In Order To Satisfy The "Foregone-Conclusion Rationale"***

During a witness interview, ask questions to satisfy the "foregone-conclusion rationale." If you are able to interview the user of the encrypted device, establish her ownership or control over it, and her ability to decrypt and access specific files thereon.

#### ***E. If All Else Fails, Compel Decryption, Not Disclosure Of The Password***

If drafting a subpoena or other compulsory process, do not command production of the password, as this will likely result in quashal. *United States v. Kirschner*, 823 F.Supp.2d 665, 669 (E.D. Mich. Mar. 30, 2010). Instead, command decryption of the encrypted information and production of a decrypted version, emphasizing that you do not seek the contents of the target's mind, but only the pre-existing, voluntarily-created contents of the target's media.

#### ***F. Act Quickly***

People sometimes forget passwords.

## **IV. Conclusion**

#### ***A. Exhaustively Investigate The Sought-After Records to Render Encryption Irrelevant***

In light of *Doe*, the foregone-conclusion rationale is the most promising basis for compelling decryption. Satisfy it by identifying the records sought, their location, who controls them, and their authenticity, with as much specificity as possible. As encryption technology evolves to render compelled decryption more difficult,<sup>3</sup> it will become even more important to identify precisely what was encrypted in the first place, and who can decrypt it.

<sup>3</sup>Sebastian Anthony, *Unbreakable crypto: Store a 30-character password in your brain's subconscious memory*, EXTREME TECH (July 19, 2012), <http://www.extremetech.com/extreme/133067-unbreakable-crypto-store-a-30-character-password-in-your-brains-subconscious-memory> (last viewed August 26th, 2012)

<sup>4</sup>Travis Korte, *Biometric Identification Will Replace Many Passwords In Next Five Years, says IBM*, THE HUFFINGTON POST (Jan. 4, 2009) ([http://www.huffingtonpost.com/2011/12/30/biometric-identification-\\_n\\_1177277.html](http://www.huffingtonpost.com/2011/12/30/biometric-identification-_n_1177277.html)).

If you cannot satisfy the foregone-conclusion rationale, but have evidence of encrypted documents and a party's ability to decrypt them, then compel production of the documents and immunize only the act of decryption. Although the *Doe* court rejected this approach, it did so after concluding that there was no evidence that the encrypted media contained anything. However, if the *Doe* court had instead found that *Doe's* media contained voluntarily-prepared records and granted them Fifth-Amendment protection due to their encryption, then the court would have departed from the Supreme Court precedent described above.

The contents of a combination safe are not immune from subpoena because the owner of the safe must use her mind to turn the dial. *Doe* would have had to use his mind to decrypt the documents, but the Government immunized him for any testimonial aspects of this act of decryption. In your arguments, draw a bright line between the unprotected documents on the one hand, and the act of decryption on the other: as the documents are non-testimonial, only the decryption need be immunized. The Fifth Amendment protects the contents of the mind, but not the voluntarily-prepared contents of digital media, even if they are encrypted.

#### ***B. The Rise Of Biometrics***

There is a somewhat new technology that can protect sensitive data without keeping that data from appropriate consideration by the justice system. Moreover, it offers better protection from attackers than password-based encryption. This technology is biometrics.<sup>4</sup>


Biometrics is a branch of biology that measures and analyzes biological data, so that a person's biological properties—rather than her password—could be used to grant her secure access to an information system.

The advantages of biometrics over passwords are obvious: rather than encrypt using a string of characters that one could forget, or that could be captured by an attacker, biometrics are based on biological characteristics specific to a particular user and which cannot be as easily captured

by another. Biometric encryption can be based not only on fingerprints, DNA, and voice samples, but also retinas, and walking and typing patterns. Advances in processing speed appear to have made biometrics appropriate for everyday use.

More importantly for the justice system, biometric-based encryption alleviates the constitutional obstacles described above, because here the act of decryption—the providing of a fingerprint, voice sample, or other physical act—falls under the category of noncommunicative, and thus non-testimonial acts that may be compelled without violating the Constitution.

Congress can take advantage of this heretofore-overlooked distinction. It could mandate the use of biometrics in federal procurement to ensure that federal employees and contractors cannot conceal misconduct or contraband from the justice system by invoking the Fifth Amendment in relation to their encryption. In the criminal context, bail or plea agreements, along with supervised release conditions, could bar the use of password-based encryption. Courts and parties considering plea agreements, probation officers drafting supervised-release conditions, along with any attorneys drafting contracts, should consider barring the use of password-based encryption, so that all parties can have access to all information should disagreements arise.

While biometric encryption may be a win-win both for information security and the functioning of the justice system, only time will tell whether it will produce a preferable result for society, or generate its own, currently-unforeseen problems. 



**Subscribe To THE FEDERAL EVIDENCE REVIEW to keep current on the latest evidence cases and issues**

The Annual Subscription Is Less Than \$25 Per Month. (That's \$295 per year)

Learn more at: [federalevidence.com/subscribe](http://federalevidence.com/subscribe)

**Author:** James Silver received a B.A. from Stanford University, and a J.D. and M.A. from Duke University. He is a Trial Attorney in the Computer Crime & Intellectual Property Section of the Criminal Division of the U.S. Department of Justice, and was a principal author of the government's brief in *Doe*. He served as a law clerk, worked in the private sector, and then prosecuted child-exploitation offenses on behalf of the Department. Any views expressed herein are his own, and not necessarily those of the Department.

### The Evidence Viewpoints® Series

**Series Purpose:** Evidence Viewpoints® provides a forum for judges, practitioners, and scholars to discuss and address topical evidence matters.

**Writing An Evidence Viewpoints Article:** The Federal Evidence Review accepts the submission of articles for publication. For more information on submitting an article, see <http://federalevidence.com/submissions>

**Reprints Available:** Article reprints may be requested. Upon publication of a work in the Federal Evidence Review, the author or others may order a reprint file for the work for a standard fee. The PDF reprint may be printed or distributed (including on a website or by email) or used for training, conferences or newsletters. The PDF reprint may a useful vehicle for circulating evidence ideas, as well as for current or potential clients or other audiences. For more information on reprints, contact:

[Submissions@FederalEvidence.com](mailto:Submissions@FederalEvidence.com)