Compelled Production of Plaintext and Keys

Phillip R. Reitinger
Phillip.Reitinger@chicagounbound.edu
Compelled Production of Plaintext and Keys

Phillip R. Reitingert

While many features of computer networks that may adversely affect privacy are outside of an individual's control, the ability to encrypt information may provide computer users with near absolute privacy for the content of their communications and stored data. In part for this reason, privacy advocates suggest that universal, strong encryption is a bulwark against the intrusion of government into personal privacy. Effective protections come at a price, however, because absolute privacy also protects criminals. Law enforcement, quite naturally, prefers a solution that protects privacy while preserving its present ability to gain access to data and communications, when authorized by law, to protect the public.

This Article will not attempt to resolve this somewhat theological debate, which depends to a great degree on whether one

† Trial Attorney, Computer Crime and Intellectual Property Section, Criminal Division, Department of Justice. The opinions expressed in this Article are those of the author and do not necessarily reflect the opinions of the Department of Justice or the United States Government.

I would like to thank the following individuals for their thoughts, advice, and assistance (not all of whom have reviewed this Article): Scott Charney, Marty Stansell-Gamm, Steve Mitchell, Peter Toren, Alex White, Don MacPherson, Robert Litt, Geoffrey Greiveldinger, Gail Thackery, and Don Ingraham.


2 Law enforcement has frequently suggested that the use of cryptography will impair its ability to intercept communications pursuant to a judicially authorized “wiretap” under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, 18 USC §§ 2510-22 (1994). See Kent, Codes, Keys, and Conflicts at 20 (cited in note 1). A greater threat to law enforcement's ability to protect the public, however, may arise from the inability of law enforcement to access encrypted electronically stored material, uncovered, for example, while executing a search warrant.

3 "Considered from a law enforcement perspective, what is needed is strong cryptography that protects the nation's communications infrastructure but that does not simultaneously imperil the government's ability to comprehend intercepted communications—when law enforcement comes armed with a court order." Kent, Codes, Keys, and Conflicts at 20 (cited in note 1).

4 I am indebted to Daniel Weitzner of the Center for Democracy and Technology for framing the issue in this way.

171
believes, as a first principle, that absolute privacy is a social good. Instead, it will assume the continued availability and expanding use of strong, non-key-escrowed encryption. In such a world, the ability of law enforcement to obtain access to encrypted evidence will depend largely on its ability either to compel the production of a key or password necessary to decrypt encrypted material or to compel the production of the plaintext of that material from its holder. This Article will examine, therefore, the legal issues raised by law enforcement’s attempts to gain access to plaintext and keys.

The principal legal obstacle to compelling production of keys is the Fifth Amendment privilege against self-incrimination, which provides that no person “shall be compelled in any criminal case to be a witness against himself.” This Article will examine the application of the privilege against self-incrimination to the production of keys or plaintext, principally in the context of a grand-jury subpoena. Part I discusses how

---

5 While a few short years ago encryption was unknown to criminals and law enforcement, in 1994 the FBI’s Computer Analysis and Response Team (“CART”), which is responsible for forensic analysis of computers seized by that agency, reported encountering encryption in 2 percent of its cases. Conversation between the author and Mike Noblett, Unit Chief, CART, FBI (April 9, 1996).

6 “Key escrow encryption” involves the storage, or “escrow,” of keys or key components with third parties. “Non-key escrow encryption” involves the storage and maintenance of keys by users/owners.

7 This Article generally uses the term “key” to mean any key, password, or similar access device. In some instances, in accord with common practice and as indicated in context, “password” will be used to mean a sequence of characters used to control access to a hardware or software system, like a password for a computer network, while “key” will be used to refer specifically to encryption and decryption keys.

8 “Plaintext” is unencrypted or decrypted text; “ciphertext” is encrypted text.

9 US Const, Amend V. Other practical problems may hamper governmental compulsion of keys. Even if the Fifth Amendment does not authorize the recipient of a subpoena or other legal request to withhold a key, the recipient can always claim that the key was lost, or even intentionally destroyed, before receipt of the subpoena or request. While a court could reject such a claim and order production, enforceable via contempt, in many situations proof of the continued existence of the key will be impossible, rendering encrypted information unavailable to law enforcement. See Part III.D.

10 The conclusions contained in this Article are also applicable to other legal demands for information, including requests for production, FRCP 34, and civil subpoenas, FRCP 45. These methods will be discussed at points, but because the focus of this Article is on the ability of law enforcement to gain access to keys and plaintext, it will concentrate on grand-jury subpoenas.

In addition, this Article will not address the Fifth Amendment implications of compelling disclosure of keys as part of any mandatory key-escrow regime. For a discussion of the Fifth Amendment issues involved in such a regime, see A. Michael Froomkin, The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution, 143 U Pa L Rev 709, 833-838 (1995); Note, The Clipper Chip: Cryptography Technology and the Constitution, 21 Rutgers Computer & Tech L J 263, 280-81 (1995).
keys function as intangible locks on electronic documents. Part II addresses compelling the production of encrypted documents in plaintext form and concludes that a grand-jury subpoena can direct the production of the plaintext of encrypted documents, although a limited form of immunity may be required. Finally, Part III addresses compelling the production of keys, and concludes that, similar to the production of plaintext, a grand-jury subpoena may direct the production of documents that reveal keys. In either case, the Fifth Amendment does not protect the contents of voluntarily prepared, nonprivate documents, including plaintext and keys. Rather, the privilege only protects the "act of production," and then only in some cases. Part III also suggests that whether law enforcement can compel production of keys that are only known, rather than recorded, is an open question, but one that should arise infrequently because most keys will be recorded.

I. KEYS TO INTANGIBLE LOCKS

If I have a document with important information that I wish to keep secret, I have a number of options. I could memorize the information and destroy the document, but then, of course, I may lose the information if my memory fails or is imperfect. I could lock the document in a safe or hide it in a secure place. I could store it on a computer that requires a password. Or, I could encrypt it.

Passwords provide one type of intangible lock. Instead of storing the document in a safe, I store the document on a computer that requires entry of a password for access. Without the key, I cannot readily use the computer and the documents it contains. However, as with storing the document in a safe, which is vulnerable to someone who can crack the safe, a technician could probably analyze the computer (more specifically, the hard disk) and obtain the information anyway, although perhaps only with considerable effort.

Encryption provides a more robust intangible lock. While a lengthy discussion of how encryption and other access-control methods work is beyond the scope of this Article, a short review helps frame the debate about compelled decryption. In brief, encryption involves the encoding of material so that it is not

---

11 For an encyclopedic treatment of the subject, see Bruce Schneier, Applied Cryptography (John Wiley & Sons, Inc., 1994).
understandable unless decoded. The material to be protected is processed using a particular algorithm, which usually depends on a key as a second input, resulting in an encrypted document. The key is a binary number that is used by an algorithm as a necessary part of the encryption or decryption process. In some cases, the same key is used for encryption and decryption, while in others, different keys are used. For example, the widely used Data Encryption Standard ("DES") algorithm uses a single key fifty-six bits in length—up to more than 70,000,000,000,000,000,000 in decimal notation—for both encryption and decryption. Public-key algorithms use different keys for encryption and decryption, and much longer keys, such as 512 (and greater) bit numbers—over 150 decimal digits. For many algorithms, longer keys make “breaking” the encryption scheme more difficult. Thus, typical implementations of encryption, particularly public-key encryption, will involve extremely long keys.

The keys themselves are meaningless sets of binary digits. While there may be numeric constraints on the numbers chosen—for example, they may have to be generated from prime numbers—these numbers have no semantic content. In addition, although a person could in some circumstances select a key that

---

12 An encryption scheme need not use a key, but could depend on the secrecy of the algorithm itself. For example, reversing all the letters in a message—changing “this is a footnote” to “etontoofasisiht” is a form of encryption, if a very poor one. Encryption algorithms that depend on the secrecy of the algorithm alone for security generally are not secure, and are less likely to be used than key-based systems.

13 The key, which can vary in length, could be limited to certain characters, such as alphanumeric characters. In the world of computers, however, the key would still be represented in the computer as a binary number.

14 For example, if one encrypts a message by rotating each letter in the alphabet up one letter, so that the message “subpoena” becomes “tvcqpfob,” the algorithm is the rotation cipher, and the key is one. If the cipher were limited to alphabetic characters, it would repeat if the key became larger than twenty-five because rotating twenty-six letters is the same as rotating zero letters, rotating twenty-seven letters is the same as rotating one letter, and so on. In other words, the key can run from zero to twenty-five in decimal numbers, or from 00000 to 11001 in binary numbers. Therefore, the key has a maximum length of five bits, although not all keys of five bits can be used—keys 11010 (decimal twenty-six) through 11111 (decimal thirty-one) are duplicates of keys 00000 (decimal zero) through 00101 (decimal five).

15 One of these keys is publicly known (the “public key”), while the other is kept secret (the “private key”). Keys for public-key algorithms are frequently longer than for secret-key algorithms because public-key algorithms depend on the difficulty of solving particular mathematical problems, which become more difficult as the size of the numbers involved increases.

16 A 1,024 bit key, for example, is roughly 146 alphanumeric characters. Mark Eckenwiler, Net.Law, NetGuide 39 (Nov 1995) (available online at http://www.panix.com/~eck/5th-amdt.html).
had meaning to that person—for example, choosing “Imguilty”\textsuperscript{17}
as the key to encrypted documents about a robbery\textsuperscript{18}—the semantic content of the key is immaterial to its use for encryption or decryption. That is, the meaning is not used in the encryption or decryption process, the key could just as easily be “xyzqzxtg”. In sum, while the key might arguably have content (albeit arbitrary content), it has no necessary meaning.

Encryption is a more robust intangible lock than passwords or safes because proper implementation of secure cryptographic algorithms provides practically unbreakable security for encrypted material. With a sufficiently robust algorithm, a secure implementation, and a sufficiently large key length, no one could decrypt the document (given current computing power) in time for the information contained in the document to be useful, at least not without expending an unduly high amount of time and resources.\textsuperscript{19} Someone who obtained a copy of my encrypted document would have all of my critical information right before her but would be unable to read it. In fact, I could publish my encrypted document in the newspaper, and only someone with the decryption key could understand it.

II. OBTAINING PLAINTEXT

A. The Obligation to Produce Plaintext

Because decryption of a document can be impracticable without a key, a governmental entity seeking access to my information must either obtain the key or compel production of my information in plaintext form. The latter is straightforward. First, assume I have custody of a plaintext document. Obviously, the government (or civil litigants) can compel production of that document (assuming appropriate standards are met) through a

\textsuperscript{17} The phrase “Imguilty” could be made a DES key by changing each letter into its seven-bit American Standard Code for Information Interchange (“ASCII”) representation and concatenating them (that is, making them a continuous string), for a total of eight seven-bit letters, or fifty-six bits, which is a standard DES key.

\textsuperscript{18} See Greg S. Sergienko, Self Incrimination and Cryptographic Keys, 2 Richmond J L & Tech 1, ¶ 9 (1996) (available online at http://www.urich.edu/-jolt/v2i1/sergienko.html).

\textsuperscript{19} For example, one could attack the Rivest-Shamir-Adleman (“RSA”) algorithm by attempting to factor one of the numbers involved in the algorithm, the “modulus.” If the modulus is a 664-bit number, a network of one million computers, each capable of performing one million steps per second, would take almost four thousand years to factor the modulus. Schneier, Applied Cryptography at 284 (cited in note 11).
document request\textsuperscript{20} or a subpoena.\textsuperscript{21} That I physically lock that
document in a safe is not material; so long as the document is in
my custody, I must produce it in response to a legally authorized
demand.

The result should not differ if, instead of locking the docu-
ment in a safe, I lock the contents through encryption. Put anoth-
er way, how I choose to secure a document in my possession
cannot justifiably control its discoverability. Therefore, even if I
store the document on a computer that requires a password for
access, I must produce the document when faced with an autho-
rized demand. Similarly, if I encrypt the document, I should be
required to produce the unencrypted version if I receive an au-
thorized demand for the same.

The legal status of encrypted documents should be no differ-
ent from any other machine-readable or machine-translatable
records, such as unencrypted records stored on a computer in a
special format that renders them indecipherable without special
software and/or hardware. Any subpoena for computer data re-
quires the respondent to access binary data and print out Eng-
lish, numbers, and so on, because the respondent must produce
records in \textit{usable} form in response to a document request\textsuperscript{22} or a
subpoena. For example, I could not respond to a request by pro-
ducing a “hex dump”\textsuperscript{23} of information from a spreadsheet or
word-processing program if the meaning of the data were avail-
able to me. Encryption is analogous; the producing party will
have special hardware or software that translates the data into
usable form for that party. The plaintext remains available to the
producing party, and so it also remains available to other parties

\textsuperscript{20} FRCP 34.
\textsuperscript{21} FRCP 45; FRCrP 17.
\textsuperscript{22} FRCP 34 defines “documents” as including “other data compilations from which
information can be obtained, translated, if necessary, by the respondent through detection
devices into reasonably usable form.” FRCP 34(a). In addition, the Advisory Committee’s
Note states:

Rule 34 applies to electronic data compilations from which information can be
obtained only with the use of detection devices, and \ldots when the data can as a
practical matter be made usable by the discovering party only through
respondent’s devices, respondent may be required to use his devices to translate
the data into usable form.

\textit{Proposed Amendments to the Federal Rules of Civil Procedure Relating to Discovery}, 48

\textsuperscript{23} Typically, a printout of binary data stored on a computer appears in hexadecimal
form, which prints one character per four binary digits.
in civil litigation and to law enforcement in criminal investigations.  

One might argue to the contrary that, unlike storing a document on a password-protected system, encryption creates a new document, and that courts cannot require recipients of demands for documents to recreate a destroyed plaintext document. For example, I could translate the document into a foreign language and destroy the original. Could a subpoena for documents or a document request demand that I produce a plain English version? The answer, perhaps, is no; one could view the translation into the foreign language as creating a new document that is subject to discovery, but the old destroyed document is no longer in my custody or control. Of course, even under these circumstances, the information contained in the document could still be discovered through deposition, trial, or grand-jury testimony.

In the battle of analogies, however, encryption is far more like storing a document on a computer or locking it in a safe than translating it. Translation, at least when performed by a human being, involves the application of human reasoning and communication to a complex problem, and can alter meaning or change nuances easily. Translation also serves a purpose other than mere security, namely, communication. Encryption, on the other hand, is a purely mechanistic process that does not of necessity add, subtract, or alter information, and which serves the primary purpose of security. In these regards, encryption is

24 In McDonnell v United States, 4 F3d 1227, 1244 (3d Cir 1993), the government, citing NLRB v Sears, Roebuck & Co., 421 US 132, 162 (1975), argued that it need not decode documents from 1934 to produce the plaintext in response to a Freedom of Information Act ("FOIA") request, because the decoding would create a new document, and an agency is not required to create documents to respond to a FOIA request. In response, the court stated, "we are not persuaded that translation [that is, decoding] of existing documents would be tantamount to imposing on the Government the burden of creating records." McDonnell, 4 F3d at 1244. Note that decrypting recently encrypted documents imposes even less of a burden because the decryption can be accomplished by software rather than manually.

25 See Braswell v United States, 487 US 99, 121 (1988) (Kennedy dissenting) ("A subpoena does not, however, seek to compel creation of a document; it compels its production.").

26 For a contrary analysis, see Greg S. Sergienko, Self Incrimination and Cryptographic Keys, 2 Richmond J L & Tech 1, ¶ 30 (available online at http://www.urich.edu/~jolt/v2il/sergienko.html) (cited in note 18).

27 Information, such as date and time, could be added intentionally during the encryption process, but this is not necessary and, in any event, adding such information does not change the meaning of the document.

28 Encryption could compress a document as an incidental part of the process, but, again, this does not change the meaning of the document.
like locking a document in a safe, or storing it on a computer, while translation is not.\textsuperscript{29}

Therefore, if law enforcement subpoenas information that I have encrypted, I must produce the information in plaintext if it remains available to me in that form, assuming I have no other proper objection, such as my privilege against self-incrimination.

B. Plaintext and the Privilege Against Self-Incrimination

1. \textit{Documents and the privilege against self-incrimination.}

As noted, the government can compel the production of plaintext. In response, the recipient of a subpoena for plaintext might assert the Fifth Amendment privilege against self-incrimination. However, because voluntarily prepared documents generally are not subject to this privilege, such a claim would be invalid. Instead, the critical question is whether the act of producing the documents implicates the privilege.

Voluntarily prepared documents rarely, if ever, implicate the privilege against self-incrimination. The Fifth Amendment applies only to communications that are (1) compelled; (2) incriminating; and (3) testimonial.\textsuperscript{30} Assuming that the subpoenaed plaintext is incriminating, it is still not privileged because a voluntarily prepared document\textsuperscript{31} does not contain compelled testimonial evidence.\textsuperscript{32} In \textit{Fisher v United States},\textsuperscript{33} for example, the Supreme Court held that production of accountants’ workpapers relating to two taxpayers, when the papers were in the possession of the taxpayers’ attorneys, did not offend the taxpayers’ privilege against self-incrimination, because the workpapers did not contain compelled testimonial evidence. Such a subpoena “does not compel oral testimony; nor would it ordinarily compel the taxpayer to restate, repeat, or affirm the truth of the contents

\begin{itemize}
\item \textsuperscript{29} If, however, the translation were performed by machine, then it is likely that a subpoena for documents in the original text would be proper.
\item \textsuperscript{30} \textit{Fisher v United States}, 425 US 391, 408 (1976) (stating that the privilege against self-incrimination “applies only when the accused is compelled to make a testimonial communication that is incriminating” (emphasis in original)).
\item \textsuperscript{31} Note that if decryption created a “new” incriminating document, this analysis would not apply. Compulsion to create a new incriminating document violates the Fifth Amendment. See \textit{SEC v College Bound, Inc.}, 849 F Supp 65, 68 (D DC 1994); \textit{Bertucci v Cunningham}, 1984 WL 1213, *5 (SD NY); \textit{FTC v Singer}, 534 F Supp 24, 26 (ND Cal 1981), aff’d, 668 F2d 1107 (9th Cir 1982). As noted above, however, decryption does not create a “new” document, but simply makes available the original one. See Part II.A.
\item \textsuperscript{33} 425 US at 408-410.
\end{itemize}
of the documents sought.\textsuperscript{34} That is, no testimony is compelled—only the act of production itself: "In the case of a documentary subpoena, the only thing compelled is the act of producing the document."\textsuperscript{35}

However, despite the rationale of Fisher, the Supreme Court has left open the possibility that some private papers may be protected under the privilege against self-incrimination.\textsuperscript{36} While a complete review of the relevant cases is beyond the scope of this Article,\textsuperscript{37} many recent decisions considering the issue have determined that the privilege does not protect the content of voluntarily prepared papers, even if personal.\textsuperscript{38} In any case, any protection of documents as personal, private papers will not rest on whether they are encrypted—except insofar as relevant in

\textsuperscript{34} Id at 409.
\textsuperscript{35} Id at 410 n 11.

\textsuperscript{36} See id at 401 n 7, 414 (explicitly not resolving privilege as to private papers); Boyd v United States, 116 US 616, 634-35 (1886) (establishing protection of private papers under both the Fourth and the Fifth Amendments).

\textsuperscript{37} A number of articles discuss this matter, including Kenneth J. Melilli, Act-of-Production Immunity, 52 Ohio St L J 223, 237-38 n 94 (1991); Robert P. Mosteller, Simplifying Subpoena Law: Taking the Fifth Amendment Seriously, 73 Va L Rev 1, 5-6 n 10 (1987); Samuel A. Alito, Jr., Documents and the Privilege Against Self-Incrimination, 48 U Pitt L Rev 27, 54 (1986) ("[T]he logic of [Fisher and Doe I] leaves no room for distinctions between types of preexisting, voluntarily prepared documents." (footnote omitted)).

\textsuperscript{38} See In re Grand Jury Proceedings, Subpoenas for Documents, 41 F3d 377, 379 (8th Cir 1994) (stating that the Fifth Amendment does not protect voluntarily created private business and financial papers); In re Grand Jury Subpoena Duces Tecum Dated Oct 29, 1992, 1 F3d 87, 93 (2d Cir 1993) (collecting cases, cert denied, 114 S Ct 920 (1994); In re Sealed Case, 877 F2d 83, 84 (DC Cir 1989) (stating that privilege does not cover the contents of voluntarily prepared personal records); In re Grand Jury Proceedings on Feb 4, 1982, 759 F2d 1418, 1420 (9th Cir 1985) (holding contents of personal financial documents not privileged); Senate Select Committee on Ethics v Packwood, 845 F Supp 17, 23 (D DC 1994) (holding contents of personal diaries not protected by Fifth Amendment), stay denied, 114 S Ct 1036 (1994); Doe I, 465 US at 618 (O'Connor concurring) ("the Fifth Amendment provides absolutely no protection for the contents of private papers of any kind."); Melilli, 52 Ohio St L J at 237-38 n 94 (cited in note 37) (noting that court decisions continuing to find protection for the contents of private papers are "irreconcilable" with the compulsion requirement as construed by Fisher). But see United States v McCollom, 651 F Supp 1217, 1222 (ND Ill 1987) (stating that contents of private papers are protected only where compelled disclosure would intrude upon "the heart of our sense of privacy," if at all), aff'd, 815 F2d 1087 (7th Cir 1987); A. Michael Froomkin, The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution, 143 U Pa L Rev 709, 836 (1995) (cited in note 10) (stating that Boyd has "residual vitality for nonbusiness, nonfinancial, private papers and documents that are kept in the home . . . ."); Mosteller, 73 Va L Rev at 5-6 n 10 (cited in note 37) ("After Doe [I], the scope of potential protection apparently has been narrowed to cover only the contents of personally prepared, non-business, intimate private documents."); Comment, Confusion among the Courts: Should the Contents of Personal Papers be Privileged by the Fifth Amendment's Self-Incrimination Clause?, 9 St John's J Legal Commentary 219, 232-41 (1993) (analyzing, by circuit, the status of the contents-based privilege).
determining that the documents are private—but rather on the nature of the plaintext in the documents.

2. The act-of-production doctrine.

That the plaintext itself is not privileged does not end the inquiry because the "act of production" may be compelled, testimonial, and incriminating even if the documents produced are not. In Fisher the Court noted:

The act of producing evidence in response to a subpoena nevertheless has communicative aspects of its own, wholly aside from the contents of the papers produced. Compliance with the subpoena tacitly concedes the existence of the papers demanded and their possession or control by the [recipient]. It also would indicate the [recipient's] belief that the papers are those described in the subpoena. 39

Whether these "tacit averments" are testimonial and incriminating generally depends on the facts and circumstances of each case. 40 If a subpoena is involved, the act of production will, of course, be "compelled." Therefore, if the act of producing the documents in response to a subpoena is testimonial and incriminating, the government must immunize the person producing the documents to prevent use of the protected aspects of the act of production. 41

The definitions of the terms "testimonial" and "incriminating" merit some discussion. The Court defines "incriminating" rather broadly. The definition covers evidence "which would furnish a link in the chain of evidence needed to prosecute . . . ." 42 However, the hazard of incrimination must be "substantial and 'real,' and not merely trifling or imaginary . . . ." 43

The term "testimonial" is more complex, but appears to refer to the communication of information 44 from the mind of the person claiming the privilege. For example, forcing a person to sign

---

40 Id.
41 See Part II.B.4.
43 Marchetti v United States, 390 US 39, 53 (1968). See also Fisher, 425 US at 412 (noting that the threat of incrimination must be "realistic").
44 "[I]n order to be testimonial, an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information." Doe v United States, 487 US 201, 210 (1988) (footnote omitted) ("Doe II").
a consent form allowing access to unidentified foreign bank accounts is not testimonial because it does not communicate any information to the government. And many compelled activities are not testimonial because they do not extract information from the mind of the witness, but from his body (including compelling a witness to provide handwriting or voice exemplars) or from third parties. Finally, the “testimonial” element is subject to a de minimis exception: the compelled act must be “sufficiently testimonial” to implicate the privilege.

In Fisher, the Court identified three ways in which an act of production can implicitly communicate incriminating facts: it can (1) concede the existence of a document; (2) concede possession, location, or control of a document; and (3) assist in authentication of a document. The Court examined each of these types of communications to determine if the act of production in that case was both testimonial and incriminating and thus subject to the Fifth Amendment privilege.

With respect to existence and possession, the Fisher Court held that because the existence and location of the documents sought were “foregone conclusions,” the act of production was not

---

45 In Doe II, the Court affirmed a district-court order requiring a person to sign such a consent form:

We read the directive as equivalent to a statement by Doe that, although he expresses no opinion about the existence of, or his control over, any such account, he is authorizing the bank to disclose information relating to accounts over which, in the bank’s opinion, Doe can exercise the right of withdrawal.

Id at 217-18.

46 See Pennsylvania v Muniz, 496 US 582, 590-91 (1990) (noting in a drunk-driving case: “The physical inability to articulate words in a clear manner due to the lack of muscular coordination of [the defendant’s] tongue and mouth . . . is not itself [testimonial].”).


49 Requiring a witness to sign a consent form, for example, does not force him “to reveal, directly or indirectly, his knowledge of facts relating him to the offense or to share his thoughts and beliefs with the Government[,]” but merely “facilitates the production of evidence by someone else . . . .” Doe II, 487 US at 213, 213 n 11 (emphasis added) (footnote omitted).

50 Fisher, 425 US at 411. For example, although “[w]hen an accused is required to submit a handwriting exemplar he admits his ability to write and impliedly asserts that the exemplar is in his writing[,]” these acts are not “sufficiently testimonial” to invoke the Fifth Amendment. Id.

51 Id at 410-13. See also Froomkin, 143 U Pa L Rev at 835 (cited in note 10) (“If the act of handing over the papers is noncommunicative—that is, if it neither reveals the existence of the document nor authenticates it—then the Fifth Amendment ordinarily does not apply.” (footnote omitted)); Mosteller, 73 Va L Rev at 7 (cited in note 37).
testimonial. The workpapers were prepared not by the taxpayer, but by the accountant, who could testify about them, and their existence and possession were already clearly established.\textsuperscript{52} In other words, even if an act of production conveys information to the government on these issues, it is not testimonial unless the information is new, or unknown, to the government in a material way.\textsuperscript{53} While courts disagree as to the showing required to establish a foregone conclusion,\textsuperscript{54} the most recent statement from the

\textsuperscript{52} Fisher, 425 US at 411-412.

\textsuperscript{53} Id at 411 ("[T]he taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers"). The Court's "foregone conclusion" analysis was criticized by Justice Brennan:

I disagree . . . that implicit admission of the existence and possession or control of the papers in this case is not "testimonial" merely because the Government could readily have otherwise proved existence and possession or control in these cases.

Id at 428 (Brennan concurring in the judgment). See also Charles G. Geyh, The Testimonial Component of the Right Against Self-Incrimination, 36 Cath U L Rev 611, 635 (1987) ("Assessing whether a suspect has been compelled to testify in light of what he has been compelled to testify serves only to muddy fifth amendment analysis." (emphasis in original)). In other contexts, whether information is protected by the privilege against self-incrimination does not turn on whether the information is cumulative. For example, even if the government has a videotape of a suspect committing a robbery, with his fingerprints on the weapon, so that his commission of the crime is a foregone conclusion, the government still cannot compel the suspect to state whether he committed the crime.

Mosteller explains that the foregone-conclusion theory is justified as a restriction on the "testimonial" element, because when an implicit communication is involved, as in a communication associated with an act of production, "it is necessary to consider whether the government is really asking a 'question' through the subpoena." Mosteller, 73 Va L Rev at 32 (cited in note 37). Note that because the communication is implicit in the act of production, the government cannot avoid asking the question if it is to obtain the information it requires through the production of the document. Mosteller argues that if the government knows the answer to the implicit question and is uninterested in the response, then the unnecessary question and answer should not violate the Fifth Amendment. Id. See also Melilli, 52 Ohio St L J at 239-41 n 96 (cited in note 37).

Alternatively, the foregone-conclusion theory is also explained by the scope of act-of-production immunity, which is discussed below. See Part II.B.4. In brief, act-of-production immunity only protects against the use (including derivative use) of the testimonial and incriminating aspects of the act of production. However, if there is an alternate source for the evidence, then it is not tainted and the evidence may be used. Kastigar v United States, 406 US 441, 461 (1972). When the existence or possession of the document, for example, is a foregone conclusion, there is an alternate source for these elements, and a grant of immunity need not preclude their use. In other words, under a "foregone conclusion" analysis, if the prosecution can show in advance that an alternate source exists for what might otherwise be immunized testimony, the prosecution, in effect, can hold a Kastigar hearing in advance of compulsion, greatly reducing the burden on the prosecution because it need not show an alternate source for all its evidence. See Mosteller, 73 Va L Rev at 33 n 107 (cited in note 37).

\textsuperscript{54} Compare United States v Fox, 721 F2d 32, 37-38 (2d Cir 1983) (requiring that evidence must "eliminate any possibility" of incrimination), with Butcher v Bailey, 753
Supreme Court indicates that the fact revealed by the act of production must be one the government can "readily establish."^{55}

The *Fisher* Court also found that even if the act of production had minimal testimonial significance about existence and possession, it was not incriminating because:

surely it is not illegal to seek accounting help in connection with one's tax returns or for the accountant to prepare workpapers and deliver them to the taxpayer. At this juncture, we are quite unprepared to hold that either the fact of existence of the papers or of their possession by the taxpayer poses any realistic threat of incrimination to the taxpayer.^{56}

This portion of *Fisher* appears to suggest that admitting existence or possession of a document through an act of production is not incriminating unless the existence or possession of the document, standing alone and apart from the document's contents, is incriminating.^{57} Subsequent cases, however, have held that conveying information about the existence of documents can be incriminating if the contents of the document are incriminating.^{58}

F2d 465, 469 (6th Cir 1985) (finding that "no serious doubt" was sufficient). See also United States v Stone, 976 F2d 909, 911 (4th Cir 1992) (finding it a foregone conclusion that the owner of a beach house would possess utility bills and rental records for it), cert denied, 113 S Ct 1843 (1993); Day v Boston Edison Co., 150 FRD 16, 21 (D Mass 1993) (finding that the act of producing an alleged illegal tape recording would incriminate plaintiff where the defendant only "strongly suspec[ed] the existence of the tape"); Melilli, 52 Ohio St L J at 239-41 n 96 (cited in note 37).

*Baltimore City Dept. of Social Services v Bouknight*, 493 US 549, 555 (1990) (finding that a mother could not claim that the act of producing her son was privileged merely because the production would establish his existence and authenticity, where the state could "readily establish" the same). Interestingly, in *Bouknight*, the Court, although not using the words "foregone conclusion," treated the concept as applying to the incrimination rather than the testimonial element of the privilege. Id. In this regard, commentators disagree on whether the foregone-conclusion analysis should relate to whether a communication is testimonial or whether it is incriminating. Compare Mosteller, 73 Va L Rev at 30-33 (cited in note 37) (arguing that foregone-conclusion analysis may eliminate the testimonial element of the act of production but not the incrimination element), with Geyh, 36 Cath U L Rev at 635-36 (cited in note 53) ("The issue of what a suspect may be compelled to attest to is addressed by the incrimination requirement.").


See Mosteller, 73 Va L Rev at 19-20 n 57 (cited in note 37). If existence or possession alone were required to be criminal, only subpoenas for items such as handguns used in crimes or contraband would implicate the privilege.

See United States v Argomaniz, 925 F2d 1349, 1356 (11th Cir 1991) (finding that compliance with an IRS summons would inform the government of the existence of documents establishing unreported income and that the summons violated the privilege);
and conveying information about possession or location can be incriminating if that information assists in proving a criminal case. Although this issue remains in flux, for the privilege against self-incrimination to protect against the admission of existence or possession inherent in an act of production, the act of production must, at a minimum, convey new information re-

United States v Edgerton, 734 F2d 913, 921 (2d Cir 1984) (holding that oral testimony about the existence of financial records was incriminating because any responsive answer would tend to increase the likelihood of success of a prosecution for failure to file a tax return); Fox, 721 F2d at 36-38 (holding that act of producing papers unknown to the government may be incriminating and is protected by the privilege); McCollom, 651 F Supp at 1222-23 (stating that subpoena that would reveal the existence of documents concerning accounts unknown to the government would be testimonial and incriminating). See also Mosteller, 73 Va L Rev at 26-27 (cited in note 37) (arguing that revealing the existence of an incriminating document is necessarily incriminating). But see United States v Aeilts, 855 F Supp 1114, 1119 (CD Cal 1994) (holding act of producing financial records testimonial and incriminating).

However, the apparent holding of Fisher, that mere existence (apart from the contents) of documents must be incriminating for the privilege to apply, has support. See In re Grand Jury Proceedings (Martinez), 626 F2d 1051, 1055 (1st Cir 1980) (stating that the existence of documents "in most cases will be so trivial that the Constitution is not implicated"); Stephen A.盐茨堡 and Daniel J. Capra, American Criminal Procedure 474 (West, 4th ed 1992) (stating that the existence of documents must be incriminating independent of their content for this part of the act-of-production analysis to apply). See also Resolution Trust Corp. v Lopez, 794 F Supp 1, 2 (D DC 1992) (noting that the mere act of production is unlikely to incriminate unless the purpose of the investigation is to establish ownership or existence of the papers demanded) (citing Office of Thrift Supervision v Zannis, 1990 WL 421186 (D DC)).

See Argomaniz, 925 F2d at 1356 (holding privileged the act of producing documents establishing unreported income); United States v Cates, 686 F Supp 1185, 1193 (D Md 1988) (holding privileged the act of producing copies of W-2 forms and deposit slips because they would be evidence that the recipient of the subpoena possessed information from which he should have determined his taxes). As with existence, however, the apparent holding of Fisher that mere possession (apart from the contents) of documents may be incriminating has support. See Saltzburg & Capra, American Criminal Procedure at 474 (cited in note 58) (stating that control of document must be incriminating independent of its content). Mosteller has argued that "compelled admission of possession violates the fifth amendment only when possession in and of itself is testimonially incriminating," such as when possession is a crime, tends to establish prior criminal possession, shows guilty knowledge, or helps to authenticate by tying an item to the producing party. Mosteller, 73 Va L Rev at 25-26 (cited in note 37). Note that some of these types of incrimination, including showing guilty knowledge, depend on the content of the produced item.
garding existence or possession, and that new information must be “realistically” incriminating.

As for authentication, the Fisher Court did not separately discuss the testimonial and incriminating nature of any communications. Instead, the Court stated that production would merely express “the taxpayer’s belief that the papers are those described in the subpoena.” On the facts of Fisher, this was not sufficiently testimonial and incriminating to require immunity; because the taxpayers did not prepare the papers and could not vouch for their accuracy, they could not authenticate the papers. Therefore, there was no substantial threat of testimonial incrimination from any implicit admission of authenticity—put another way, the producing party’s conclusion about responsiveness had no real significance.

In most cases involving documents, “present” existence or possession will not be incriminating if the government can establish prior existence and possession. For example, if the government knows a suspect received bank records concerning a known account, revealing that those records continue to exist and that he currently possesses those records poses no realistic threat of incrimination, given the government’s knowledge of prior existence and the link between the document and the suspect already established by proof of prior possession. Indeed, if present existence and possession need be shown, then nearly every act of production would be incriminating, because rarely can the government prove that an individual did not destroy the subpoenaed records seconds before the subpoena arrived. Compare Mosteller, 73 Va L Rev at 25-26 (cited in note 37) (arguing that such a broad interpretation of the privilege would violate Fisher’s holding).

In United States v Rue, 819 F2d 1488, 1492-94 (8th Cir 1987), the court misunderstood this distinction. The court held that, to demonstrate that existence and possession are foregone conclusions, the government must show existence and possession on the date that the legal demand for the documents is made. Id at 1493. While continued existence and possession are burdens the government may have to shoulder to obtain enforcement, compare United States v Rylander, 460 US 752, 760 (1983) (noting a “presumption of continuing possession” stemming from an enforcement order), in most cases such facts pose no realistic threat of incrimination if the existence or possession of the documents at any time is a foregone conclusion. For example, existence, possession, and authenticity are foregone conclusions when the government can obtain testimony from an entity that it previously had possession of the documents and transferred them to the person claiming the privilege. See Thomas v Tyler, 841 F Supp 1119, 1131 (D Kan 1993). In a few other cases, however, present existence or possession, or lack thereof, may be incriminating.


Id at 412-13.

Id. This portion of Fisher has been criticized as an improper statement of the law of evidence because the taxpayers’ testimony could help to authenticate the documents by admitting that the produced documents were the accountants’ workpapers. See Mosteller, 73 Va L Rev at 16-17 (cited in note 37).

The probative value of the workpapers depended on their accuracy, which required testimony from the accountants, making the taxpayers’ admissions insubstantial. Mosteller, 73 Va L Rev at 17-18 (cited in note 37). See also Fisher, 425 US at 413 (“Without more, responding to the subpoena in the circumstances before us would not appear to represent a substantial threat of self-incrimination.”). For this reason, Fisher is probably best read as holding that the testimonial admissions regarding authenticity were not in-
Like admissions of existence and possession, communications regarding authenticity involve highly fact-sensitive determinations and can require a specific examination for testimonial and incriminating aspects. Expressing a belief that "the papers are those described in the subpoena" can be testimonial if the response calls for an exercise of independent judgment that reveals facts. Demanding "documents concerning illegal transactions" from a suspect would provide an extreme example because by producing documents in response, the suspect would be testifying that the documents concerned illegal transactions. If communications regarding responsiveness do not reveal new facts, however—if authenticity is a foregone conclusion—then the implicit communications are not testimonial. In sum, like communications regarding existence and possession, if the implicit communications regarding responsiveness reveal new facts and if those new facts are "realistically" incriminating, the communications can implicate the privilege against self-incrimination.

---

65 Fisher, 425 US at 413.

66 "In general, a subpoena compels testimonial conduct under the fifth amendment whenever it requires the witness to make a discrimination between documents and thereby to provide identifying information that is relevant to authenticity." Mosteller, 73 Va L Rev at 12 (footnote omitted) (cited in note 37). See also In re Grand Jury Proceedings, 41 F3d at 380 ("[T]he broader, more general, and subjective the language of the subpoena, the more likely compliance with the subpoena would be testimonial." (citations omitted)); Fox, 721 F2d at 39-40 (holding that an act of production that is sufficient to authenticate the documents produced is testimonial even if the records were not self-prepared); United States v Porter, 711 F2d 1397, 1401-02 (7th Cir 1983) (determining that "implicit authentication" of documents is compelled testimony).

67 See Bouknight, 493 US at 555 (stating that a mother could not claim that the act of producing her son was privileged merely because the production would establish his authenticity where the state could "readily establish" the same); In re Grand Jury Subpoena Duces Tecum Dated Oct 29, 1992, 1 F3d at 93-94 (holding that production of a calendar was not protected where prior production of an edited version of the calendar established its existence and authenticity); Melilli, 52 Ohio St L J at 239-42 n 96 (cited in note 37) (noting that the "prevailing view . . . appears to be that the government's specification of an alternative means of identification renders authentication a foregone conclusion"). Compare Doe I, 465 US at 614 n 13 (finding risk of incrimination from production "substantial and real" where the government failed to produce independent authentication evidence); Mosteller, 73 Va L Rev at 29 n 92 (cited in note 37) (noting that while the Fisher Court applied the foregone-conclusion concept only to possession and existence, the Doe I Court suggested the government could also use the concept to resist the defendant's authentication claim).


69 Some have suggested that any production of self-prepared documents requires a grant of immunity, at least unless the authenticity of the documents is a foregone conclusion, because the act of production is sufficient to authenticate the documents. See In re Grand Jury Proceedings (Martinez), 626 F2d at 1055-58 (requiring immunity for production of documents prepared under defendant's direction, even though the government

The act-of-production analysis should apply to subpoenas for decrypted text just as it does to subpoenas for material that has never been encrypted. If the government does not know that the material it asks a defendant to produce is encrypted, and the material is to be produced in decrypted form, then the act of production is identical to producing any other material. One merely applies the act-of-production analysis to the act of producing the plaintext document, just as if the document had been stored in a safe.

Moreover, the fact that the government knows the material was stored only in ciphertext\(^7\) will almost never affect whether that act of production is privileged. Producing the plaintext of a document known to be encrypted may indicate, in addition to the existence, possession, and authenticity of the plaintext,\(^7\) the present ability to decrypt the encrypted document; that is, production of plaintext may indicate present possession of the key associated with the document at issue.\(^7\)

Proof of present possession of a key associated with an encrypted document, however, will rarely affect whether producing that document in plaintext is testimonial, even if one believes that present possession of a key

---

"probably" could authenticate the records independently); *In re Grand Jury Proceedings*, 41 F.3d at 380 (determining that competency to authenticate documents depends on who prepared them). But see *In re Kave*, 760 F.2d 343, 356 (1st Cir 1985) (noting that self-preparation is not a requirement). Another court stated the issue this way: "if authentication is not a foregone conclusion, [the] act of authentication would be incriminating—as a link in the chain of evidence—only if the nature of the documents indicated that their contents might be incriminating." *Butcher*, 753 F.2d at 470 (footnote omitted).

\(^7\) The material must be stored only in ciphertext (encrypted form) because if it is also stored in plaintext, then the material can be produced from that source. The government must also know the material is stored only in ciphertext, or the production conveys no information that is not already conveyed when any plaintext document is produced.

\(^7\) With regard to existence and possession of the document, production of decrypted text indicates the existence and possession of the produced information just as production of never-encrypted material. In either case, production indicates present ability to access. With respect to authentication of that document, production indicates only that the recipient believes the documents produced are those called for in the subpoena, just as in production of never-encrypted material.

\(^7\) Present possession of the key is the only material fact indicated by the act of producing plaintext in this situation. First, authentication of the key is immaterial if the government is not seeking to introduce the key—which it is not if it has not subpoenaed the key. Second, the government already knows about the use of encryption (we assumed that the government knew the document was stored only in encrypted form) and, therefore, existence of a key and/or algorithm is a foregone conclusion. Thus, all the government learns (of a possibly incriminating nature) from production of plaintext is that the recipient of a subpoena currently possesses the key and/or algorithm necessary to access the material.
proves a stronger connection between the document and the producer than mere production of the plaintext.

To prove this point, consider two hypothetical fact patterns. First, assume that the act of producing the plaintext is testimonial and incriminating apart from proving present possession of the key. In such a case, immunity for the act of production is required, and that immunity protects against use of the act of production to prove possession of the key. Second, assume that the act of producing the plaintext is not testimonial and incriminating. In this case, proof of possession of the key rarely will be material. Proof of possession of the key primarily demonstrates a connection between the document and the possessor of the key, and that fact is probably neither testimonial nor incriminating, because if it were both then the act of producing the plaintext itself would be testimonial and incriminating, which is contrary to our assumption.\(^7\)

Proving present possession of the key associated with a document is most important if the government can use that "testimony" to demonstrate some incriminating fact other than those already proven by the act of producing the document in plaintext. This testimony will normally have little value,\(^7\) and, in most cases, what little possession of the key proves will not be incriminating.\(^7\) Possession of the key could, however, be incriminating

\(^7\) For example, assume that I have prepared a spreadsheet recording my income, and that document is responsive to a government subpoena. My act of producing that document may be testimonial because my production concedes existence of the statement and assists in authenticating it—proof of present possession is important under these facts only because it helps authenticate the document. That information may be incriminating if the contents of the statement help to incriminate me. But see notes 56-61 and accompanying text. If the government can prove by independent evidence that I keep such a record, however, and can authenticate it without my act of production—for example, perhaps another witness saw me edit the document and recalls the exact figures on the spreadsheet—then the existence and authenticity of the statement are foregone conclusions and the act of production is not testimonial.

Assume now that the government knows that I keep my records in encrypted form. In the first situation, where existence and authentication are not foregone conclusions, my act of producing the document in plaintext proves existence and helps establish authenticity, and the government must immunize my act of production. Therefore, the government cannot use any element of my method of producing the document against me, including the fact that I decrypted the document. See Part II.B.4. And in the second situation, because existence and authentication of the document are foregone conclusions, proof of possession of the key is immaterial because the existence of the document and my connection to it are foregone conclusions.

\(^7\) If the key is stored in tamper-resistant hardware, production might also indicate exclusive possession of the key, much like production of a unique item or document, such as a document under seal. In contrast, use of a "private" key does not indicate exclusive possession because a private key can be shared.

\(^7\) This analysis presumes that the use of encryption is not illegal. If the government
if the government were to use that fact to show possession or control over other encrypted documents not involved in the act of production, such as other encrypted documents the government had previously seized. This situation could be treated as if the subpoena were a specific demand for a key, and so should be evaluated as discussed in Part III, which considers demands for production of keys.

4. The scope of act-of-production immunity.

Here again, little difference exists between encrypted documents and unencrypted documents. The scope of immunity should be the same for the plaintext of encrypted documents as for never-encrypted documents. Therefore, when subpoenaing plaintext, a prosecutor should consider, in advance, the applicability of the act-of-production doctrine and possible alternative sources for any communications inherent in the act of production.

If the act of production is testimonial and incriminating, the government cannot compel production without offering act-of-production immunity to the party receiving the subpoena, whether the information subpoenaed is stored in plaintext or ciphertext form. In United States v Doe ("Doe I"), the government had issued a subpoena to Doe seeking copies of his businesses' contracts, bank records, accounting records, and other business records. Because the district court found that the act of producing the documents would compel the owner to admit that the records existed, that he possessed them, and that they were authentic, the Supreme Court affirmed the lower courts' holdings that the act of production was testimonial self-incrimination. Accordingly, the Court held that, in order to compel Doe to produce the records, the government would have to request use immunity through the statutory mechanism for compulsion of testimony.

But what is the scope of this immunity, and how does it limit the government? The answer is still subject to considerable dispute. In one view, the grant of immunity covers only the testimonial and incriminating aspects of the act of production, and never

---

can learn through the act of production that the recipient of a subpoena currently possesses an illegal encryption program, production of plaintext might well be testimonial and incriminating apart from the content of the document produced.

77 Id at 613-14.
78 18 USC §§ 6001 et seq (1994).
prevents the use of the unprivileged contents of the subpoenaed document. This theory relies on language in *Doe I*, in which the Court stated:

Respondent argues that any grant of use immunity must cover the contents of the documents as well as the act of production. We find this contention unfounded. To satisfy the requirements of the Fifth Amendment, a grant of immunity need be only as broad as the privilege against self-incrimination . . . . As discussed above, the privilege in this case extends only to the act of production. Therefore, any grant of use immunity need only protect respondent from the self-incrimination that might accompany the act of producing his business records.80

Similarly, the First Circuit has held:

[A] grant of immunity to the [claimant] which precluded subsequent government use of the fact of his compliance with the subpoena would not preclude subsequent government use of the contents of the surrendered documents.81

The Department of Justice takes a similar view that the contents of documents are not protected by act-of-production immunity.82

---

80 Id at 617 n 17 (internal citations omitted).
81 *In re Grand Jury Proceedings (Martinez)*, 626 F2d at 1058. See also *In re Grand Jury Proceeding, Special Apr 1987*, 890 F2d 1, 4 (7th Cir 1989) (determining that future derivative use of the contents of documents is not prohibited but derivative use of the act of production is prohibited); *Butcher*, 753 F2d at 470 n 7 (noting that even if the act of production conveys information concerning authentication, the contents of the documents can be used in criminal proceedings if the documents can be independently authenticated); *Porter*, 711 F2d at 1403 n 4 (noting that the contents of documents are not testimony and so are not within the immunity created by 18 USC § 6002); *McCollom*, 651 F Supp at 1223 (finding it unlikely that act-of-production immunity precludes the use of the contents of documents whose existence is known). But see Sergienko, 2 Richmond J L & Tech at ¶¶ 27-28 (cited in note 18).
82 The United States Attorneys' Manual indicates:

If immunity is sought for the limited purpose of obtaining records pursuant to [Doe I], that fact should be clearly stated in the application for immunity. Examination of a witness who is compelled to produce records in such cases should be sufficient to determine whether there has been compliance with the subpoena, but care should be taken to limit inquiries to matters relevant to the act of producing the records since all such testimony, and leads therefrom, will not be usable against the witness. The contents of the records may, of course, be used for any purpose because they are not privileged.
Under this view, then, only the testimonial and incriminating aspects of the act of production are protected. In other words, one first determines whether the act of production has testimonial and incriminating aspects that require a grant of immunity, and, if so, then the grant of immunity precludes use of those particular aspects. Derivative-use immunity also applies to such testimony—meaning that if the testimonial and incriminating aspects of the act of production lead the government to other evidence, the government may not use that evidence either. However, because the contents are never privileged, they can provide an alternate source for the existence, possession, or authenticicity of the document. For example, the contents of the documents might make the document self-authenticating.

Other courts and commentators, however, believe that in some circumstances use of the contents of subpoenaed documents is prohibited. Under this view, although the contents are not privileged, use of the contents can be tainted by the immunized act of production. For example, under this theory, if the government is ignorant of the existence of documents, granting act-of-production immunity may preclude it from any use of the subpoenaed documents.

One commentator has suggested that prosecutors must treat the subpoenaed documents as appearing magically in the grand-jury room, so that the act of production has no effect adverse to the person producing the documents. See Alito, 48 U Pitt L Rev at 60 (cited in note 37). But this may overread the privilege, because the grant of immunity need not cover nontestimonial aspects of the act of production. If existence of the documents is a foregone conclusion, the grant of immunity need not protect against the use of the proof of existence inherent in the act of production.

In Kastigar, 406 US at 456-59, the Supreme Court held that the government could compel incriminating testimony only if it granted a witness immunity from both direct and derivative use of that testimony.

See Melilli, 52 Ohio St L J at 245-46 (cited in note 37) (describing this theory).

See In re Sealed Case, 791 F2d 179, 182 (DC Cir 1986) ("The fact that the contents of the tapes are unprivileged does not mean that they will necessarily remain untainted."). (emphasis in original)).

See McCollom, 651 F Supp at 1222-23 (refusing to order the production of information associated with unknown bank accounts, even though the government offered act-of-production immunity, because such information could not be used against the producer either directly or derivatively); Mosteller, 73 Va L Rev at 44-47 (cited in note 37) (arguing that if the government is ignorant of the existence of documents, granting act-of-produc-
Under either view, the consequences of granting act-of-production immunity could be considerable.\textsuperscript{88} If the government
provides immunity for the act of production, under *Kastigar v United States* the government would face the burden in a prosecution of the immunized witness of proving that none of its case was derived from the immunized testimony, even if the contents of subpoenaed records can be used against the witness. This can be a difficult burden under any circumstances, even when the act of production conveys little information. Similarly, in one case in which act-of-production immunity was provided under 18 USC § 6002, the court stated:

> Should the government decide to prosecute [the party claiming the privilege] following the grand jury investigation, it will be prohibited from any use of the testimonial aspects relating to [the claimant’s] compelled act of producing the documents against him. As noted in a similar case by then-Judge Scalia, the government would “have to meet the ‘heavy burden’ of proving that all evidence it seeks to introduce is untainted by the immunized act of production.”

Even for direct use alone, the burdens imposed by act-of-production immunity could be considerable. For example, if the government obtains a document under a grant of act-of-production immunity, the document must be authenticated without the assistance of any immunized testimony, which may be difficult.

---

use any testimonial act implicit in production against all but the custodian it selects.

Id at 130 (Kennedy dissenting). However, the majority’s statement above is best seen as recognition that the burden of proving an independent source is considerable even when a grant of immunity protects only a limited amount of testimony.

406 US at 460-62.

But see *United States v Tapert*, 1993 WL 168923, *4 (6th Cir), cert denied, 114 S Ct 442 (1993) (refusing to reach the question, raised for the first time on appeal, of whether the district court should have held a *Kastigar* hearing because the defendant produced documents under a grant of act-of-production immunity).

*United States v North*, 920 F2d 940, 942-43 (DC Cir 1990), reflects how difficult this burden can be. In *North*, which was not an act-of-production case, prosecution witnesses had seen Oliver North’s immunized congressional testimony, although the prosecutor had not. Because those witnesses had seen immunized testimony, which could have indirectly shaped their testimony, the Court found that the Fifth Amendment had been violated. Id at 942-43. See also Akhil Reed Amar and Renee B. Lettow, *Fifth Amendment First Principles: The Self-Incrimination Clause*, 93 Mich L Rev 857, 877-80 (1995).

In re *J.W.O.*, 940 F2d at 1167 (internal citation omitted) (quoting *In re Sealed Case*, 791 F2d at 182).

See *McColom*, 651 F Supp at 1223 (holding that the government must resort to
5. Collective entities.

If the subpoenaed party is a collective entity, such as a corporation, partnership, or labor union, the government need not offer act-of-production immunity. In *Braswell v United States*, the Court made clear that if the records are subpoenaed from a collective entity, as opposed to an individual or a sole proprietorship, then the custodian must produce the records without a grant of act-of-production immunity. Because the act of production is an act of the collective entity, which has no privilege against self-incrimination, the custodian merits no protection even if the act of production would personally incriminate him. Simply put by the Court, "[a] custodian may not resist a subpoena for corporate records on Fifth Amendment grounds," unless, perhaps, he is the sole employee and officer of the corporation. Despite extensive criticism, this is still the law.

Means other than the act of production, such as handwriting exemplars, to authenticate the document); Mosteller, 73 Va L Rev at 41 (cited in note 37) (noting that, to avoid this problem, the government may set out in advance the sources it will employ to authenticate any documents produced in response to the subpoena).

Difficulties can exist even if the contents of a document provide an independent source of evidence:

[A] grand jury subpoenas Mr. X’s bank records and receives records pertaining to a previously unknown and unnamed account. Since Mr. X’s immunized act of production furnishes the only evidence linking him to this account, the attorneys and investigators conducting the investigation cannot follow up on this information in any way.

Alito, 48 U Pitt L Rev at 63 (cited in note 37).


See *Doe 1*, 465 US at 617 (holding act of production of sole proprietorship privileged).

*Braswell*, 487 US at 110.

113. See also *In re Custodian of Records of Variety Distributing, Inc.*, 927 F2d 244, 247-48 (6th Cir 1991) (denying privilege to custodian of corporate records); *United States v Dean*, 989 F2d 1205, 1206 (DC Cir 1993) (denying privilege to custodian of government records).

Although the *Braswell* Court held that act-of-production immunity was not required, it did confer a form of immunity on the custodian. The government could “make no evidentiary use of the ‘individual act’ against the individual.” *Braswell* 487 US at 118. See also *Dean*, 989 F2d at 1209-10 (holding that government custodian’s act of production could not be used against her at trial). This form of immunity, however, allows the use of the corporation’s act of production against the individual, *Braswell*, 487 US at 118, and provides no protection from derivative use.

*Braswell*, 487 US at 118-19 n 11 (leaving open the question of whether the act of production would be testimonial and incriminating “when the custodian is able to establish, by showing for example that he is the sole employee and officer of the corporation, that the jury would inevitably conclude that he produced the records”). Some circuits have subsequently answered this open question in the negative. See *Stone*, 976 F2d at 912 (col-
III. OBTAINING THE KEY

That a party may compel production of plaintext does not mean it can actually obtain production of plaintext in every case. The government may have obtained, through authorized interception, an encrypted conversation for which there is no recorded plaintext or ciphertext except that held by the government. A person could also encrypt a document, send it to another, and then destroy both the ciphertext and the plaintext. Or a person could encrypt a document with a public key, and then destroy the plaintext, so that only someone with the private key could decrypt the document. In such situations, the government may seek to compel production of keys in order to obtain plaintext.

In this regard, stored keys are as producible as any other type of information. In civil proceedings, if necessary to translate a document, keys may be "reasonably calculated to lead to the discovery of admissible evidence." Similarly, a grand jury's subpoena power is quite broad. Thus, if the key is written down, it could be obtained through a document request or a subpoena for documents. If the key is known but not written, it could be obtained through interrogatory or compelled "testimony," assuming the privilege against self-incrimination does not apply.

A. Compelling Production of a Key and the Privilege Against Self-Incrimination

The government should be able to require the production of keys under the same conditions as if it were seeking to compel the production of plaintext, because production of keys is, for the most part, equivalent to the act of producing the decrypted docu-

---

90 Some commentators have criticized the collective-entities doctrine based on Fisher and Doe I. See Mosteller, 73 Va L Rev at 59-61 (cited in note 37); Alito, 48 U Pitt L Rev at 68 (cited in note 37). But Braswell reaffirmed the doctrine, if doing little further to justify it. Accordingly, the collective-entity doctrine lives on.

100 FRCP 26(b)(1).

101 See United States v Dionisio, 410 US 1, 8 (1973) (holding that a grand-jury subpoena for voice exemplars, which are not privileged, was not required to meet standard of reasonableness).

102 Whether or not providing a key is "testimonial" is discussed in Part III.B.

ment. Unlike other documents, the key is not sought for its meaning—a key has no substantive meaning at all. Instead, the government would seek production of a key because, like the act of producing a plaintext document, production of a key allows access to the plaintext document. For example, if the government seizes a ciphertext document in the course of a search or intercepts it, and then subpoenas the key, it seeks the key not for its meaning (what it proves) but because the key allows access to the ciphertext document. The key is a reified "act of production." Moreover, producing the key associated with that ciphertext document tends to convey the same facts, if any, associated with producing that same document in plaintext, namely the possession and authenticity of that document. The government need not introduce the key itself into evidence, because it proves nothing; rather, the government could use possession of the key to prove the possession or authenticity of the underlying document, if that were in dispute.

Therefore, in most cases, the key should be producible by granting the same degree of immunity required to obtain production of the plaintext document associated with the key. In addition, proving that no act-of-production immunity is required for the production of the key should be even easier, because the existence of the underlying document that the government possesses is, of necessity, a foregone conclusion. Moreover, the government generally can establish the authenticity of the underlying document and possession of it by showing how it obtained the document—through search and seizure, interception, and so on—so these also may be foregone conclusions. Therefore, act-of-production immunity should be necessary, if at all, only because possession of the key tends to demonstrate a connection

---

104 See note 17 and accompanying text.
105 In certain cases, the government might seek a key for purposes other than allowing access to documents.
106 Alternatively, the government could subpoena ciphertext and the associated key simultaneously. Under these circumstances, a court would first have to analyze whether the production of the encrypted text was testimonial and incriminating under the standards discussed above. See Part II.B.2. The court would then need to determine if production of the key was testimonial and incriminating under the standards discussed in this part of the text.
107 If the party could make a realistic claim that it did not have the key and so did not "possess" the plaintext, act-of-production immunity might be required if possession of the plaintext were incriminating.
between the possessor of the key and the underlying document.\textsuperscript{108}

Because keys have an independent existence, however, one must treat them as separate, producible objects. Applying current act-of-production doctrine to production of keys is quite complex. The following attempts to disentangle the doctrinal knots.

B. Recorded Keys and the Privilege Against Self-Incrimination

I will begin with a recorded key. A recorded key is a voluntarily prepared document and, therefore, does not contain compelled testimonial evidence.\textsuperscript{109} Because the content of the key is not privileged,\textsuperscript{110} as with the compelled production of plaintext, one must analyze whether the act of producing the key is testimonial and incriminating with regard to the existence, possession, or authenticity of the key itself. When one treats a key as a separate document, then the ciphertext document encrypted with the key is relevant only insofar as its incriminating character may make the act of producing the key incriminating.\textsuperscript{111}

Most often keys will be sought to unlock the contents of a document. The most obvious way in which the act of producing the key can be testimonial and incriminating under these circum-

\textsuperscript{108} The inference would be that because the subpoenaed party possesses the key, the document came from and was possessed, in plaintext form, by that party. Of course, this could be established by the content of the document itself, which would be an independent source. See Kenneth J. Melilli, Act-of-Production Immunity, 52 Ohio St L J 223, 245 (1991) (cited in note 37) (describing one view).

\textsuperscript{109} See notes 30-35 and accompanying text. It is difficult to see how a key could constitute a protected private paper, assuming that doctrine retains some validity, see note 38, because it reveals nothing about individual feeling and thought. See Bellis v United States, 417 US 85, 91 (1974). But see A. Michael Froomkin, The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution, 143 U Pa L Rev 709, 834 (1995) (cited in note 10) ("The required disclosure of the chip key resembles the required disclosure of a private paper . . . .").

\textsuperscript{110} The fact that a recorded key allows access to an encrypted document does not mean that the key contains compelled testimony any more than the key to a safe deposit box does. It is the content of the key (again, not the meaning, because the key has no meaning) that allows access. The content is not compelled testimony. Thus, the fact that the key allows access to an incriminating encrypted document does not alone require providing immunity.

\textsuperscript{111} For example, a voluntarily prepared document identifying the location of a piece of physical evidence is incriminating, but is not compelled testimony as a matter of law. The act of producing that document can be testimonial and incriminating, but the incriminating character of the physical evidence identified does not, standing alone, make it so, nor is the nature of the physical evidence revealed relevant to this inquiry. See Baltimore Dept. of Social Services v Bouknight, 493 US 549, 555 (1990) ("[A] person may not claim the Amendment's protections based upon the incrimination that may result from the contents or nature of the thing demanded." (citations omitted)).
stances is through the act's capacity, as discussed above, to link the possessor of the key to the incriminating encrypted document. The act of producing a key can be testimonial because it assists in proving the authenticity of the key and that the producer possesses it. Proof of possession is of primary importance because it helps tie the key to the producer—that it is one of "her" keys. Proof of this tie may be incriminating because the fact that an individual's key decrypts a document could, depending on the other facts involved, indicate that the individual could have accessed, authored, read, or possessed that document. In short, the fact that the producer's key decrypts the document generates an inference that it is her document. In addition, the fact that an individual knows which key decrypts a document may be incriminating because it helps to authenticate the ciphertext document, although this problem can be avoided in part by a properly worded subpoena. Note that these facts re-

---

112 As explained below, existence of the key will rarely be in question. See notes 119-23 and accompanying text.

113 The authenticity of the key is important only if the government must introduce the key into evidence for some reason. Moreover, as explained below, if the government can prove, independent of my act of production, that I possess the key associated with a particular document, then the key can be authenticated by alternative means. See note 118 and accompanying text.

114 See Bouknight, 493 US at 555 (noting that implicit control at the moment of production over a child the court had ordered be produced might aid the government in its prosecution); Eckenwiler, NetGuide at 40 (cited in note 16) (noting that the fact that you have the key that permits access to documents describing a conspiracy is powerful evidence of your participation); Froomkin, 143 U Pa L Rev at 837 (cited in note 10) (noting that the disclosure of the key by the Clipper encryption chip "is not testimonial, save insofar as it ties a particular conversation to a particular pair of chips"). In this regard, a key is like a combination to a safe. Assume, for example, the government finds a safe during the course of a search, breaks into it, and finds an incriminating document that says "I killed Jane." The government thereafter subpoenas the combination to the safe. Although a written copy of the combination is not privileged, the act of producing the combination incriminates the recipient of the subpoena, because it indicates custody and control of, or at least access to, the document, and helps to authenticate the document.

115 The fact that the key decrypts the document (producing intelligible plaintext) is strong evidence of possession and/or access, because it is unlikely that the use of an improper key would derive intelligible plaintext from ciphertext. Accordingly, if the use of a key results in intelligible plaintext, particularly for text messages, one can generally be certain that the key is the right one and that the content of the document has been correctly decrypted. Moreover, because some of the plaintext in the document may be known (standard file headers, for example), the key will be verifiable, because only one key will produce that plaintext.

116 The subpoena should not call for the exercise of independent judgment, and thus testimonial communications, by the subpoenaed party. For example, a response to a subpoena that called for the key associated with a given document would indicate that the recipient of the subpoena knew which key was associated with the document. If the subpoena instead called for all keys in one's possession, however, it would not call for the
COMPELLED PRODUCTION OF PLAINTEXT AND KEYS

semble those that production of the underlying ciphertext document in plaintext would prove because both production of the plaintext and production of the key that unlocks the plaintext demonstrate the same ability to access and control the document.\footnote{Take the example discussed in note 114, where the government subpoenaed the combination to a safe in order to prove access to and the authenticity of the document in the safe. If the government had not found the safe and had subpoenaed the document directly, production of the document would prove facts similar to those proven by production of the combination to the safe, namely, that the producer had access to the document and that he may have owned the document. In each case, the act of production demonstrates that the contents of the document were within the producer's custody or control. Also, production of a key does not prove knowledge of the contents of a document any more than production of plaintext. Documents can be encrypted by a computer without having been read by the person who possesses the key and the documents.}

In many cases, then, proof of possession of a key will require granting act-of-production immunity to the individual who produces the key. Whether immunity must be granted under these circumstances will depend on whether the government can establish, as a foregone conclusion, that a person possesses a key associated with a particular document. If the government can prove that I have the key that unlocks a particular ciphertext document, then, just like any other document, my act of producing the key is not testimonial regarding possession, and the government can require me to produce the key without a grant of immunity to cover such proof.

The government can use that same proof to establish possession and authenticity of the ciphertext document, without relying on the act of production. If the government can establish, as a foregone conclusion, that a person possesses a key associated with a particular ciphertext document, then the authenticity of that key is also a foregone conclusion. The government can authenticate the key without relying on the act of production because proof of my possession of the key, combined with the fact that the key does decrypt the ciphertext, establishes that the key is what the government claims—my key to the document.\footnote{For example, assume that I send an encrypted document to a friend with a memorandum that says, "please hold this document that I have encrypted," followed by my signature. The government finds the document and memorandum and subpoenas the key. The authenticity of the key that I produce in response to the subpoena is a foregone conclusion—the fact that it decrypts the document I sent, see note 115, in combination with the memorandum, will establish the key's authenticity without reference to the act of production.}

Of course, in many cases the authenticity of the key will not be at
issue, because the government will not need to introduce the key into evidence.

Most act-of-production issues regarding keys will pertain to authenticity and possession rather than existence, which will rarely be in question. First, if the government seeks to compel production of a key, it is probably because the government already possesses a document that appears to be encrypted. Because existence of the underlying encrypted document is a foregone conclusion, the existence of a key and/or algorithm is also a foregone conclusion, and, therefore, admitting it is not testimonial. Second, unlike typical act-of-production paradigms, in which the contents of a produced document are incriminating—and, thus, revealing the document's existence may be testimonial and incriminating—admitting existence of the key will seldom convey incriminating facts. Therefore, the existence of the key will rarely be incriminating even if it is testimonial.

Finally, even if the foregoing considerations require the government to grant act-of-production immunity to compel production of a key, the scope of the immunity should be quite narrow. The contents of the key are not privileged, and it is the con-

---

119 The analysis in this part applies equally to documents describing the encryption algorithm used and to the key itself.

120 If the encrypted document were buried in another file, however, the government might not know that it possessed an encrypted file. Under these circumstances, the government would probably subpoena the plaintext rather than the key.

121 See Bouknight, 493 US at 555 (determining that if the government can readily establish existence of the subpoenaed item, then admitting its existence is insufficiently incriminating for the Fifth Amendment); United States v McCollom, 651 F Supp 1217 (ND Ill 1987) (refusing to uphold an assertion of the privilege where existence of documents relating to known accounts was a foregone conclusion), aff'd, 815 F2d 1087 (7th Cir 1987).

122 Mere existence of a key will not indicate that any encrypted incriminating information exists.

123 An interesting problem arises if the key is stored in a document responsive to the subpoena which contains other elements, and of which the government is not aware. A document might say, for example, "I have used the key '123abc' to encrypt documents revealing that I killed John." In such a case, the subpoenaed party could make a stronger claim that production revealed the existence of new incriminating documents. But one should not be able to resist production by burying a key in a document with other incriminating elements. So, if the additional incriminating facts would require granting act-of-production immunity, the immunity should extend only to those additional facts. If the prosecution does not wish to offer such immunity, the documents should be provided to the court for redaction, in camera, so that only the key will be provided to the prosecution.

124 Moreover, the contents of the key are also not tainted by the act of production. Even under the broadest acceptable view of act-of-production immunity, the contents of produced documents are privileged only if the documents' existence is unknown to the government. See note 87 and accompanying text. As explained in notes 119-23 and accompanying text, the existence of a key will rarely be in doubt.
tents that will be used to decrypt a document. Therefore, the
government can use the contents of the decrypted document
without impediment. Unless the government cannot authenticate
the document to be decrypted without using the act of production
of the key, granting act-of-production immunity should have little
effect.

Some examples are helpful. First, assume: (1) the govern-
ment seizes ciphertext documents during a search of a computer;
(2) the government also discovers during the search an encryp-
tion program that uses an extremely large key, perhaps 512 bits
or more; and (3) only one person has access to the computer. In
this situation the existence of the key is a foregone conclu-
sion—someone used one to encrypt files. Possession of the
key also may be a foregone conclusion—only one person had ac-
cess to the computer, and, therefore, that person must have
known the key if the documents were encrypted on that com-
puter. Moreover, the government can establish the existence,
possession, and authenticity of the ciphertext without the aid of
the key by presenting testimony and evidence resulting from the
search. Accordingly, the government need not use the act of pro-
duction of the key to introduce the encrypted documents into evi-
dence, and the government can establish the authenticity of the
key through proof of the authenticity of the ciphertext, combined
with the fact that the key decrypts the ciphertext. Because
the existence, possession, and authenticity of the key are fore-
gone conclusions, the court should not require act-of-production
immunity to subpoena the key from its holder.

Second, assume that the government intercepts an encrypted
communication and finds an informant who saw the sender enter
the key into her computer from a notepad at the start of the
communication. Here the existence, possession, and authenticity

125 It is not critical to meet this element that the key continue to exist. Because the
key must have existed, production does not reveal the existence of any unsuspected docu-
ment, and that the key continues to exist entails no additional incrimination. See note 60.
Moreover, the key probably is written because it is too long for most individuals to memo-
rize. Even if it were memorized, however, it still must have been recorded at the point it
was entered into the computer, when it was fixed in memory. See Part III.C.

126 Although this does not prove present possession, present possession of the key is
not itself incriminating. Possession of the key at any time is what incriminates, see note
60, and that is a foregone conclusion.

127 However, in some cases it might be reasonable to infer that the encrypted docu-
ments were created somewhere else and copied to the computer, perhaps via modem or
floppy disk.

128 See note 118.
of the key are again foregone conclusions, and, therefore, no act-
of-production immunity is required to subpoena the key from the
sender.

Third, assume the government discovers an encrypted docu-
ment during the search of a business at which a suspect works,
on a computer to which many have access. The government at-
ttempts to subpoena the key from the business, but the business
does not possess it. Although the existence of a key may be a
foregone conclusion, who possesses the key is not known. The
government cannot establish that it is a foregone conclusion that
the suspect possesses the key, and it may need to use the act of
production to introduce and demonstrate access to the encrypted
document. In short, the act of production adds to the
government's knowledge. Accordingly, act-of-production immunity
for the suspect is probably required, just as if the government
had sought to subpoena the plaintext of the document from each
of the employees. If the government can otherwise authenticate
the document, however, and tie it to the person producing the
key, the government can introduce the document in evidence
against him.

Finally, assume that the government seizes documents en-
crypted by one person ("X") with another's ("Y") public key. Other
documents seized during the search establish that Y sent the
public key to X, and what the public key was. In this case, a
subpoena directed to Y for the private key necessary to decrypt
the document does not call for any testimonially incriminating
communications, because: (1) communicating the existence of the
private key is not testimonial because it is probably a foregone
conclusion; (2) communicating possession of the private key is
not testimonial because it also is a foregone conclusion; and (3)
the key can be authenticated without reference to the act of pro-
duction by demonstrating that it decrypts documents encrypted
with the public key. Also, in this case it is highly unlikely that
production of the private key is incriminating in any fashion—the
act of producing the private key neither assists in authenticating
the encrypted document nor ties Y to the encrypted docu-

\[129\] No act-of-production immunity need be provided to the business for the reasons
discussed above. See Part II.B.5.

\[130\] The existence of a private key is necessitated by the existence of a public key,
which is part of a public-private key pair.
ment, and mere possession of a private key is not normally incriminating.

C. Unrecorded Keys and the Privilege against Self-Incrimination

An unrecorded password poses more difficulties. In general, courts will not compel oral testimony that may be incriminating. In addition, the Supreme Court has indicated in dicta that being compelled to testify about the combination of a safe implicates the Fifth Amendment.

In contrast, the Court has permitted the government to compel verbal statements that are equivalent to an act of production, and, as noted above, providing a key is equivalent to pro-

---

131 Y is not associated with the encrypted document because the document was encrypted with the public key, not the private key, and so Y may not have known about the encrypted document. Anyone with possession of Y's public key could encrypt, but not decrypt, documents using it.

132 In Curcio v United States, 354 US 118, 123-24 (1957), for example, the Court held that oral testimony by a union official about the location of records was protected by the Fifth Amendment even though the records themselves were not protected: "[The custodian] cannot lawfully be compelled, in the absence of a grant of adequate immunity from prosecution, to condemn himself by his own oral testimony." In Pennsylvania v Muniz, 496 US 582, 592-600 (1990), the Court held that a response to a question designed to determine if the respondent could remember the date of his sixth birthday, in order to determine his state of intoxication, was testimonial because the content of the answer could be used to prove intoxication. See also Giamarino v United States, 603 F Supp 820, 821 (SD NY 1985) (holding that witness could not be required to provide date of birth or social-security number); Eckenwiler, NetGuide at 39 (cited in note 16) (noting that the Fifth Amendment protects a password held only in one's head).

133 In Doe v United States, 487 US 201, 219 (1988) ("Doe II"), the Court decided that a claimant could be forced to sign a waiver that required foreign banks to release whatever account information they had concerning him. Justice Stevens, dissenting, stated that "[a defendant] may in some cases be forced to surrender a key to a strongbox containing incriminating documents, but I do not believe he can be compelled to reveal the combination to his wall safe—by word or deed." Id (Stevens dissenting). Instead of rejecting this premise, the Court accepted it:

We do not disagree with the dissent that "[t]he expression of the contents of an individual's mind" is testimonial communication for the purposes of the Fifth Amendment. We simply disagree with the dissent's conclusion that the execution of the consent directive at issue here forced petitioner to express the contents of his mind. In our view, such compulsion is more like "be[ing] forced to surrender a key to a strongbox containing incriminating documents" than it is like "be[ing] compelled to reveal the combination to [petitioner's] wall safe."

Id at 210 n 9 (internal citations omitted). Thus, in dicta, the entire Court appeared to agree that the United States could not compel a claimant to reveal a combination to a safe, which is in many ways equivalent to a key. The Court did not address the degree of immunity required.

134 In Curcio, 354 US at 125, the Court, in distinguishing prior cases, noted that a records custodian of a collective entity could be compelled to provide identification or au-
ducing an encrypted document in plaintext. Also analogous is the Court's determination that a person could be forced to sign a waiver form allowing access to foreign bank records because a key allows access to an encrypted document. It is unclear how a court would resolve these conflicting lines of authority, especially if a subpoena for an unrecorded key were directed to a custodian of corporate records. In practice, however, the government is more likely to subpoena recorded passwords than memorized ones. In many cases, keys will be far too long to be memorized, and will be stored on a computer, in encrypted form for security. But because the key is stored on the computer, albe-

thentication testimony, which "merely makes explicit what is implicit in the production itself." See also In re Custodian of Records of Variety Distributing, Inc., 927 F2d 244, 250 (6th Cir 1991) (holding that statements necessary to establish foundation of produced materials as business records could be compelled without a grant of immunity). But see In re Grand Jury Empaneled on Apr 6, 1993, 869 F Supp 298, 305-06 (D NJ 1994) (holding identification testimony compellable but not business records foundation testimony). Most instructive is the Court's treatment of this statement from Curcio in Braswell v United States, 487 US 99 (1988). The Braswell Court described Curcio as drawing a line between "oral testimony and other forms of incrimination," id at 114, the latter being subject to compulsion without immunity while the former was not. Id at 113-15. Because the Curcio Court was distinguishing cases that permitted compulsion of identification testimony, the Court's statement in Braswell suggests that verbal statements that are equivalent to those which result from an act of production are not "testimonial" for the purposes of the Fifth Amendment in the strict sense, but only to the extent that the act of production itself would be testimonial.

See Part II.A.

In Doe II, 487 US at 204-05 n 2, the government had asked the district court to order Doe to sign forms consenting to the disclosure of any bank records relating to foreign bank accounts that might exist, without acknowledging the existence of any such accounts, and stating that the forms were signed under court order. Because the consent form spoke in a "hypothetical" way, id at 215, about any accounts that might exist, the Court held that the consent form did not have any testimonial significance. Id at 219. After analyzing the terms of the form in some detail, the Court concluded:

We read the directive as equivalent to a statement by Doe that, although he expresses no opinion about the existence of, or his control over, any such account, he is authorizing the bank to disclose information relating to accounts over which, in the bank's opinion, Doe can exercise the right of withdrawal.

Id at 217-18 (internal citations omitted). Thus, the Court held that an order compelling Doe to sign the consent form did not violate the Fifth Amendment. Doe II, 487 US at 219. Indeed, as the Court noted, "it is difficult to understand how compelling a suspect to make a nonfactual statement that facilitates the production of evidence by someone else offends the privilege." Id at 213 n 11.


For example, a long key that is a sequence of arbitrary binary digits could be encrypted using a phrase that was similarly long but not arbitrary, and so could be easily memorized, like "My mother's name was Mary but she changed it." But because the phrase is long, it would make more difficult "dictionary" style attacks on the key—attacks in which
it in encrypted form, the government may subpoena it as discussed above. That is, the plaintext of a key stored in encrypted form in hardware or software is itself a document subject to subpoena—the government can compel production of the decrypted key without compelling testimony regarding the password or phrase that was used to encrypt the key. In other cases, documents reflecting an exchange of keys will exist and are subject to subpoena. Thus, only truly memorized passwords might defeat the government’s subpoena power, and the government is more likely to be able to “break” encryption if people use small, memorized keys.

D. Destruction of Keys

That the government, or civil litigants, may legally be permitted to subpoena keys will not provide access to all relevant information. Faced with the choice of providing a key that will unlock critical evidence or refusing and facing the risk, but not certainty, of contempt, many will run the risk of contempt by claiming a loss of memory or that a written key has been destroyed. One commentator has stated this point succinctly: “Where possession cannot be independently shown, common sense and experience suggest that incriminating evidence frequently will not be produced.” Thus, the only long-term, practicable solution that meets the needs of individual privacy and public security may be key-escrow encryption.

CONCLUSION

In the introduction to this Article, I stated that I would not address the greater question of the proper balance between individual privacy and public security. But I would like to close with a brief thought on the matter. The use of encryption is one of the great, virtually insoluble dilemmas of cyberspace. It provides powerful protections for privacy, but restricts the ability of law enforcement to protect the public from the depredations of criminals. The proper balance between these competing goods is not

---


139 See Part III.B.

140 Indeed, an intelligent criminal who learns of government surveillance or seizure, will, at the first opportunity, destroy any keys before receipt of a subpoena.

within the sole authority of law-enforcement professionals, nor within the special domain of privacy advocates. It is a choice for our society as a whole to make, recognizing that permitting absolute privacy will mean that law enforcement will be unable to obtain evidence in some (or many) cases, while permitting law enforcement to access keys (either through compelled production or a key-escrow regime) may mean that some individuals' privacy will be improperly invaded.

The question whether to permit law enforcement to compel production of keys arises against this background. While resolution of the proper ambit of grand-jury subpoenas for keys, and the degree of immunity required, are at the outset dry legal questions to be determined by court opinions, in the long-term such questions will be addressed popularly and legislatively as a matter of policy. In those debates, it seems to me that permitting law enforcement to compel the production of keys when necessary, with judicial supervision as appropriate, is a minimal accommodation to the need for public security in a world in which criminals have an increasing array of sophisticated tools at their disposal.

In appropriate cases, courts should order limitations on the use of keys that are subpoenaed. As the use of cryptography expands, the damage that results from improper disclosure of keys expands in like fashion. For example, a person may have used a key to encrypt large numbers of documents. Improper disclosure of the key could cause manifest harm to the owner of the key by eliminating to a considerable extent his personal and business privacy. Therefore, courts could fashion limitations on the use of subpoenaed keys, such as limiting their use to decryption of documents acquired by the government and requiring the government to keep the key confidential (consistent with law-enforcement needs), in appropriate cases. Similar types of protective orders are already familiar to courts and lawyers as part of trade-secret or employment-discrimination cases, and courts should use such mechanisms in this new field as required.