Richmond Journal of Law and Technology

Volume 2 | Issue 1 Article 3

1996

Self Incrimination and Cryptographic Keys

Greg S. Sergienko
University of Richmond

Self Incrimination and Cryptographic Keys

by Greg S. Sergienko[*]

February 13, 1996

Cite As: Greg S. Sergienko, *Self Incrimination and Cryptographic Keys*, 2 RICH. J.L. & TECH. 1 (1996) <http://www.richmond.edu/jolt/v2i1/sergienko.html>[**].

I. Introduction

{1} The Fifth Amendment commands that no person "shall be compelled in any criminal case to be a witness against himself."[1] However, extending current judicial interpretations of the Fourth and Fifth Amendments too far may allow the government easy access even to private documents, making one's diary and other documents accessible and admissible in court against their author.

{2} What the Court has taken away, technology has given. Modern cryptography can make it virtually impossible to decipher documents without the cryptographic key,[2] thus making the availability of the contents of those documents depend on the availability of the key. This article examines the Fourth and Fifth Amendments' protection against the compulsory production of the key and the scope of the Fifth Amendment immunity against compelled production. After analyzing these questions using prevailing Fourth and Fifth Amendment jurisprudence, I shall describe the advantages of a privacy-based approach in practical and constitutional terms.

II. The Fifth Amendment and the Compulsory Production of Cryptographic Keys

A. Accessibility of Documents Under the Fourth and Fifth Amendments

{3} The Fourth Amendment provides little protection from the search and seizure of documents. In *Warden v. Hayden*,[3] the Court discarded the rule that the power to search and seize depended on the assertion of a superior right to the property seized. Before *Warden*, officers could search for fruits of a crime, because a superior right was in the property owners; for contraband, because no one could legally own contraband; and for instrumentalities, because their role in the commission of the crime made them forfeitable; but could not search for mere evidence.[4] Because, for example, diaries are "mere evidence," the *Warden* rule potentially could allow search warrants to seize diaries and other purely private documents. Although *Warden* expressly refused to consider "whether there are items of evidential value whose very nature precludes them from being the object of a reasonable search and seizure,"[5] many now believe that all objects can be seized.[6]

{4} The Fifth Amendment's guarantee against self incrimination also provides little protection for existing documents. The Court generally interprets the Fifth Amendment to allow the government to compel the *production* of these documents, because the government did not compel anyone to *write* the documents.[7] Thus, the government can compel the production of documents and, if written, the key encrypting the documents. Although there may still be some protection for private documents, such protection is uncertain in its existence and narrow in its scope.[8]

{5} Under the *Warden* view and Fifth Amendment jurisprudence, written cryptographic keys cannot be distinguished from the documents themselves. If the key is found by a search, it can be used. If one can subpoena the underlying documents, one can subpoena the key.

{6} In this section, I shall assume the correctness of Justice O'Connor's belief that there is now no Fourth or Fifth Amendment obstacle to the compulsory production of existing documents, whether text, encrypted text, or cryptographic key.[9] This means that the basis of protection must be an assertion of Fifth Amendment privilege against a question asking one to disclose a memorized cryptographic key.

B. Fifth Amendment Testimoniality and the Production of a Memorized Cryptographic Key

{7} Because current law may hold that the underlying, pre-existing documents can be the subject of a search or subpoena, Fifth Amendment analysis must focus on the disclosure of the cryptographic key on the assumption that the key is not written down. The Fifth Amendment is now interpreted to bar only the production of "testimonial information,"[10] so the protection of the Fifth Amendment extends only to an incriminating communication that might "itself, explicitly or implicitly, relate a factual assertion or disclose information."[11]

{8} A non-cryptographic key is physical evidence, not testimonial evidence.[12] Thus, the Court has upheld both a Fourth Amendment seizure[13] and the compulsory production of such non-testimonial evidence, such as a blood sample[14] or the performance of sobriety tests that do not involve communication.[15]

{9} A cryptographic key need not have testimonial content. A key can be any word, phrase, or a series of randomly chosen digits. However, one can imagine a cryptographic key that has been given an incriminating, testimonial content by making it a word or phrase that confesses to a crime. Many seldom-enforced statutes[16] enable one to confess to a crime in one's cryptographic key, thereby triggering potential criminal liability and therefore the protection of the Fifth Amendment,[17] without incurring much risk of prosecution or of social obloquy should the key leak or the Fifth Amendment argument be rejected. However, many keys will not confess to a crime. So, while this may be a factor for the prudent in selecting particular cryptographic keys, it cannot be relied upon to resolve the problems before the courts.[18]

{10} Because a cryptographic key need not be testimonial and will ordinarily not be testimonial, it might be argued that the disclosure of the key could be compelled without raising Fifth Amendment issues. Why should a cryptographic key be protected from production if a non-cryptographic key such as the key to a safe, is not?[19]

{11} The difficulty in distinguishing the two cases is exacerbated by the ability of circumstances to cause the same information to be expressed in testimonial and non-testimonial ways. For example, producing a key to a safe implicitly asserts that the key I turn over is the key to the safe and implicitly admits my control over the key. These implicit admissions cannot be used against the producer of the key. However, the key itself will not be suppressed. One could easily consider the production of the key an implicit description of the shape of the key, perhaps in a standardized form common to locksmiths, in which case I have made a testimonial assertion about the key and the relation of the key so described to the safe that the key opened.

{12} Despite the functional identity between these keys, the Court has already suggested in dictum that there is a fine line that distinguishes testimonial from non-testimonial compulsion. In *Doe v. United States (Doe II)*, the Court recognized that "be[ing] compelled to reveal the combination to his wall safe" would be testimonial compulsion, but suggested that the key to a strongbox containing incriminating documents would not be.[20]

{13} The Court's conclusion in *Doe II* appears to be consistent with its other cases. The argument that the

Fifth Amendment allows the compulsory disclosure of a combination confuses the requirement that the statement be testimonial with the argument that the Fifth Amendment requires that the thing about which the statement is made be testimonial. Although the key has no testimonial content, a statement concerning the key is testimonial. The same would be true of a murder weapon. The murder weapon itself is not testimonial, but the suspect's statement about the location of the murder weapon would be testimonial. So, too, would the disclosure of the key associated with particular encrypted documents be testimonial. Thus, if a custom-designed chip included the key in hardware or firmware, the production of the chip could be compelled, just as physical evidence or a pre-existing document could be compelled.

{14} The difficulties with the boundary line the Court has drawn between testimonial and non-testimonial information are not unique to cryptographic keys. For example, although evidence about someone's physical state is not considered testimonial information, the use of heart rate and skin resistance as part of a polygraph test might well be considered testimonial. "[E]ven a subject unwilling throughout would presumably provide revealing lie-detector responses if bombarded by words meaningful in the context of the crime being investigated-'hammer!' 'club!' 'wrench!' 'pipe!'"[21] The Supreme Court suggested in *Schmerber* that the results of such a test would be inadmissible:

> Some tests seemingly directed to obtain "physical evidence," for example, lie detector tests measuring changes in body function during interrogation, may actually be directed to eliciting responses which are essentially testimonial. To compel a person to submit to testing in which an effort will be made to determine his guilt or innocence on the basis of physiological responses, whether willed or not, is to evoke the spirit and history of the Fifth Amendment. Such situations call to mind the principle that the protection of the privilege "is as broad as the mischief against which it seeks to guard."[22]

{15} Conversely, testimonial information sought not for the truth of the information, but to reveal an underlying physical state, is inadmissible under the Fifth Amendment. *Pennsylvania v. Muniz*[23] involved a videotape of someone who had been arrested for drunk driving. At one point, the defendant's interrogator asked him when his sixth birthday was.[24] The questioner was not interested in the actual date of the birthday, but in "the incriminating inference of impaired mental faculties . . . from a testimonial aspect of that response."[25] Although the inquisitor was not interested in obtaining a truthful answer, the Supreme Court held that the question implicated the Fifth Amendment.[26]

{16} These boundary lines cannot easily be extended to make disclosure of cryptographic keys non-testimonial. Ambiguities could be used to extend the Fifth Amendment to the production of implicitly testimonial conduct, such as the production of safe keys. However, to hold that an expressly assertive statement was non-testimonial would effectively eliminate the Fifth Amendment's protection against self-incrimination. A cryptographic key can be likened to testimonial statements. Consequently, it seems safe to conclude that the compulsory production of a cryptographic key implicates the Fifth Amendment.

C. The Scope of Immunity from the Compelled Production of the Key

{17} If, as the above argument suggests, the identification of the key is testimonial, the critical issue will be the extent of the immunity necessary to satisfy the Fifth Amendment's proscription of self-incrimination.[27] The federal government has suggested that it will seek to grant immunity as a tool for discovering encrypted documents.[28] Does immunity extend only to the key or does it also cover the decrypted document produced by applying the key to the encrypted text?

1. Derivative Use Immunity for Documents Produced with a Cryptographic Key

{18} The Supreme Court has distinguished between incriminating documents, which may not be protected by the privilege, and the incriminating aspects of producing the documents, from which one may claim Fifth Amendment immunity even if the documents themselves are uncovered.[29] Thus, in *United States v. Doe (Doe I)*, the Court held that the production of individual tax records in the individual's possession might have testimonial and self-incriminating aspects such that their production could only be required through a grant of use immunity.[30] Although it has been suggested that derivative immunity for encrypted documents would follow as a matter of course from the production of the key,[31] this line of cases suggests otherwise.

{19} The leading authority here is Justice White's opinion for the Court in *Fisher*, which discusses the testimonial aspects of production as though the courts could compel production so long as the amount of self-incrimination is not excessive.[32] The same sort of reasoning appears in other cases, even when those cases have resolved this analysis in favor of the individual. For example, in *Doe I*, the Court upheld a refusal to comply with a subpoena absent a grant of immunity because the incriminating effects of production were not "trivial."[33] *Doe I* distinguished *Fisher* as a case where "the act of production would have only minimal testimonial value and would not operate to incriminate the taxpayer."[34]

{20} *Fisher* did not address the issue of derivative use immunity where the government would not have found the documents without a subpoena. This is because *Fisher* involved a situation in which the government could certainly get the documents without the aid of the subpoena. "The existence and location of the papers are a foregone conclusion and the taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers."[35] Because the government did not need the subpoena to get the papers, it had sufficiently shown an independent route to the papers to make them admissible without violation of the Fifth Amendment.

{21} It is not certain that the Court still follows this narrow view of *Fisher*. In *Braswell v. United States*, a case following *Fisher*, the dissent argued without opposition from the majority that documents produced pursuant to a claim of privilege could nonetheless be used against the producer, so long as the testimonial effect of the production itself was shielded.[36]

{22} On the other hand, the Court has not held that documents compulsorily produced can automatically be used against the producer. *Fisher* does discuss the actual effect of production; the facts of the case, in which the papers were initially in the hands of the accountant, support the Court's conclusion that the production of the papers did not increase the government's information. Nothing in *Fisher*, then, can be interpreted to mean that the Fifth Amendment allows the derivative use of documents which the government could not independently find and authenticate.[37] *Doe I*, subsequent to *Fisher*, held that the documents in question need not have been produced,[38] and in the absence of a request for use immunity, the Court did not deal with the issue of derivative use immunity.[39] *Doe II*, also subsequent to *Fisher*, involved the compulsory signing of a directive to foreign banks without admitting any information.[40] Because the Court held that this did not implicate the Fifth Amendment, that case also did not involve any issue of derivative use immunity. In *Braswell* the underlying documents were corporate records and therefore not privileged,[41] so derivative use immunity could not apply.

{23} If the broad reading of *Fisher* is correct, the presumable basis for *Fisher's* apparent conclusion is that the documents themselves do not implicate the Fifth Amendment because they were not produced under compulsion. This, of course, makes perfect sense with regard to the documents considered as original objects of discovery under a search and seizure permitted by the Fourth Amendment.

{24} However, it neglects the Court's usual requirement that immunity extend to the derivative use of any compelled information. The leading case, *Kastigar v. United States*, establishes the general rule that the grant of immunity must include "derivative use immunity": immunity from "any use, direct or indirect, of the compelled testimony and any information derived therefrom . . . ."[42] *Kastigar* "prohibits the prosecutorial

authorities from using the compelled testimony in *any* respect."[43] The burden is on the prosecution, which has "the affirmative duty to prove that the evidence it proposes to use is derived from a legitimate source wholly independent of the compelled testimony."[44] Thus, use immunity expressly prohibits using testimony "as an 'investigatory lead'" or using "any evidence obtained by focusing investigation on a witness as a result of his compelled disclosures."[45]

{25} In the absence of derivative use immunity, the Fifth Amendment protection against self-incrimination places an individual compelled to produce evidence in a better position than receiving immunity. *Kastigar* relied on the Court's prior decision on state-compelled testimony, holding that "immunity from use and derivative use 'leaves the witness and the Federal Government in substantially the same position as if the witness had claimed his privilege' in the absence of a grant of immunity."[46] If the information would not have been discovered without the grant of immunity, the witness is placed in a worse position because of the grant of immunity.[47]

{26} In its cases involving the production of documents, the Court seems to have confused the issue of whether the documents are necessarily privileged with the question of whether they are the product of compelled testimonial conduct. The Court was arguably correct in its conclusion that they are not privileged because their writing was not compelled. Thus, one can conclude that if the documents had been seized as a result of a legitimate search, they would be admissible. However, the Court ignored the question of whether they were the product of compelled information. If the prosecution immunizes a defendant and asks her where the murder weapon is, and the prosecution uses that information to obtain the weapon, it will be barred from using the weapon to trace the defendant to the crime unless it can show an independent path. Indeed, the Court has recently re-affirmed its statement in *Curcio v. United States*[48] that the custodian of documents cannot be compelled to answer questions about the documents' location without a grant of use immunity.[49] Under the Court's precedents, such a grant implies that documents discovered or produced as a result of the answers to such questions would be suppressed as the product of the compelled testimony.[50] A subpoena to produce the documents implicitly requires the same information as would result from the answering of questions about the documents' location, so a distinction in the scope of derivative immunity in the two cases seems unjustified. Indeed, the Court's earlier cases expressly equate documents discovered by compulsory production and documents discovered by compulsory testimony, which then leads to the documents:

> In practice the result is the same to one accused of a crime, whether he be obliged to supply evidence against himself or whether such evidence be obtained by an illegal search of his premises and seizure of his private papers. In either case he is the unwilling source of the evidence, and the Fifth Amendment forbids that he shall be compelled to be a witness against himself in a criminal case.[51]

{27} In *Fisher* and progeny, the defendant failed sufficiently to exclude the possibility of independent discovery. So far as holdings go, as opposed to statements, there is nothing in the Supreme Court's decisions from *Fisher* to the present that excludes the possibility of its rejecting its ill-conceived and inconsistent assumptions on derivative use immunity in the case of documents. Even the statements are rare, being confined to a dissenter's assertion in *Braswell*.[52]

{28} Thus, it is still open for the Court to conclude that its conventional doctrines of use immunity apply to documentary production. In the context of cryptographic keys, that would ensure that the compulsory production of the key provided derivative use immunity for the contents of the documents decrypted with the key.

2. Immunity As a Result of the Special Properties of Cryptographic Keys

{29} Even if the Court concludes that derivative use immunity does not generally apply to documents

discovered with the aid of compelled testimony, there are special reasons for extending Fifth Amendment immunity to documents decrypted with the aid of the compelled production of a cryptographic key.

a. Creation of Communicative Content Through Decryption

{30} One unique property of a cryptographic key is that it creates communicative content. Producing an ordinary document or making available a key to a safe does not alter the communicative content of the documents produced or made available. In contrast, producing a cryptographic key gives the document a testimonial content by decrypting the document and returning it into plaintext. Thus, the compulsory production of the key is the compulsory creation of testimonial content. Without the key, the documents would not be useful as testimony.[53]

{31} Several Supreme Court opinions suggest that the creation of documentary evidence in this fashion triggers Fifth Amendment protection. The Court has held that the protection of the Fifth Amendment extends to any incriminating communication that might "itself, explicitly or implicitly, relate a factual assertion or disclose information."[54] The production of a cryptographic key indirectly relates the material contained in the document decrypted with the cryptographic key and should therefore lead to immunity under the Fifth Amendment for the document produced with the key.

{32} Elsewhere, the Court has stated that it "do[es] not view the exhibition of physical characteristics to be equivalent to the creation of documentary evidence."[55] The Court's concern with "the creation of documentary evidence" also suggests that the compulsory production of the cryptographic key, which makes possible the creation of the documentary evidence to be used in court, provides immunity as to the documents that could be created only with the key.

{33}Finally, *Fisher* and *Doe I* stated that the production sought in those cases "does not . . . ordinarily compel the taxpayer to restate, repeat, or affirm the truth of the contents of the documents sought."[56] Thus, although a person may be compelled to produce a document, compulsory production cannot require her to repeat, affirm, or explain the contents of the document. However, the compulsory production of the key does force the repetition of the document in a new and courtroom-usable form. Under these precedents, then, the compulsory production of a key should give rise to immunity from culpability derived from the document produced with the key.

{34} Even if it were argued that it is the document and the key that jointly create the testimonial content, that is sufficient, because self-incrimination protection extends to all the "links [that] frequently compose that chain of testimony which is necessary to convict any individual of a crime."[57] Thus, an ordinarily non-privileged item, such as the identity of the client or fee information, is privileged if the disclosure of the item would reveal the substance of an attorney-client communication.[58] Because the key is a necessary link in the chain, it gives rise to immunity from documents with it.

b. Authentication Through Decryption

{35} A second unique property of a cryptographic key is that it can operate as a digital signature, necessarily authenticating a document.[59] Indeed, if the person providing the information has never shared that information with anyone else, a cryptographic key provides a more effective way of authenticating than locks, because it is easier to pick locks than to decrypt without a key.[60]

{36} The Fifth Amendment precludes the compulsory authentication of documents. "[T]he Fifth Amendment may protect an individual from complying with a subpoena for the production of his personal records in his possession because the very act of production may constitute a compulsory authentication of incriminating

information."[61] "'[T]he constitutional privilege against self incrimination . . . is designed to prevent the use of legal process to force from the lips of the accused individual the evidence necessary to convict him or to force him to produce and authenticate any personal documents or effects that might incriminate him.'"[62]

{37} The Court noted that where the compulsory production of documents may authenticate them, "reliev[ing] the government of the need for authentication," the Fifth Amendment precludes their production.[63] Although *Fisher* suggested that no grant of immunity is necessary where the "possession [of the documents, their] existence, and authentication were a 'foregone conclusion,'"[64] these issues will seldom be indisputable with respect to cryptographic keys. One difference between "a pre-existing document and a pre-existing object" is that a prosecutor "can usually authenticate [a document, such as a diary,] as the defendant's either by content or handwriting analysis."[65] Authentication in this way will be impossible without the key. The impossibility of such authentication suggests that the factual premise of *Fisher* cannot apply in the case of computer-encrypted documents, so that compulsory production of a cryptographic key requires granting use immunity for the documents decrypted with the key.

3. Conclusion

{38} Close analysis of cases interpreting the Fifth Amendment suggests that the amendment does provide protection against the compulsory production of cryptographic keys. This protection can result from a reconciliation of the Court's inconsistency between the compulsory production of documentary evidence and its more general treatment of the doctrine of derivative use immunity. Even in the absence of such a reconciliation, the Court's precedents suggest that it can be expected to hold that the documents produced from a cryptographic key cannot be used against the producer of the key, because a cryptographic key authenticates and confers testimonial content on documents that are otherwise unauthenticated and meaningless.

{39} This result is quite narrow: only those who claim to be criminally incriminated by the key or the decrypted document can claim the protection of the Fifth Amendment. Although I have suggested a way in which overbroad criminal statutes can be turned to the advantage of innocent citizens,[66] this result seems unsatisfactory. Why should criminals have a right to privacy in their documents when non-criminals do not? The obvious answer is that the Fifth Amendment protects against self-incrimination, not against invasions of privacy. However, early American cases provided much broader protection for privacy. The next section justifies a revival of these early authorities.

III. The Advantages of a Traditional Solution

{40} Although early cases provided immunity from search and seizure and the compulsory production of most private documents, it is unclear whether any of this early protection for private documents survives. Justice O'Connor's concurrence in the Doe II opinion expressed her belief that the Court's opinion eliminated the possibility of protection for documents. It has been suggested that her opinion for the court in *Baltimore City Department of Social Services v. Bouknight*[67] establishes her *Doe II* concurrence as the holding of the Court.[68]

{41} On the other hand, *Bouknight* involved an attempt to conceal a child, which is quite a different case from documents.[69] The absence of protection for corporate documents results from the state's power of visitation over corporations, which meant that their records were not private.[70] The same argument would apply with even greater force with a child, which could not be said to be the private property or records of a parent. Moreover, even after the Court's decision in *Baltimore v. Bouknight*, the Court continues to say that the privilege reflects "our respect for the inviolability of the human personality and of the right of each individual 'to a private enclave where he may live a private life.'"[71] This idea of a private life is difficult to

reconcile with a privilege that applies solely to self-incriminating and testimonial conduct before a judicial tribunal.

{42} This part of the paper suggests the outlines of an alternative approach to the problem of confidential documents and justifies that approach in terms of the Constitution and its traditional interpretation. Even if the United States Supreme Court refuses to entertain such an approach, state courts may be persuaded that such an approach is both more consistent with the intent of the adopters of the Constitution and contemporary considerations of policy.

A. Search and Seizure under *Boyd v. United States*

{43} In *Boyd v. United States*,[72] the Supreme Court held that "a search and seizure [was] equivalent [to] a compulsory production of a man's private papers" and that the search was "an 'unreasonable search and seizure' within the meaning of the Fourth Amendment."[73] Under *Boyd*, the government could not search for private documents and could not compel their production.

{44} The *Boyd* decision was based on a careful review of the intent at the time of the framing and the practices of the colonial governments to which the framers objected.[74] Historically, searches could only be based on the superior property rights of the government or some other person in the things for which the search was made.[75] Thus, one could search for and seize "stolen or forfeited goods"[76] and contraband, such as "counterfeit coin, lottery, tickets, implements of gambling, & c."[77] "Forfeited goods" included the instrumentalities of the crime, which were forfeited because of their use in the crime[78] and included papers that were fruits, contraband, or instrumentalities.[79] Because mere evidence could not be searched for at the time of the framing, and the framers intended to adopt these common-law restrictions,[80] these standards defined what the framers would have understood as a "reasonable" search under the Fourth Amendment.[81]

{45} *Boyd* likewise cited the work of the first congress and contemporary rules of equity in interpreting the scope of the Fifth Amendment's right against self-incrimination.[82] The *Boyd* opinion noted that even the "obnoxious writs of assistance" did not allow searches for private papers.[83] As the *Boyd* Court further observed, the same history showed an absence of power to use process to seize private papers,[84] and the first Congress expressly adopted chancery practice, which forbade the compulsory production of documents.[85] Congress did not enact a statute that could possibly be construed to allow the seizure of private papers, whether for use in evidence or in forfeiture, until 1863.[86] The *Boyd* Court concluded from this review of practices of the framing that the compulsory production of private papers or a search for them violated the Fifth Amendment as well as the Fourth Amendment.[87]

{46} *Boyd*'s antiquity suggests that it is consistent with the framers' intent. Indeed, both *Boyd* and the subsequent *Gouled* decision expressly placed their analysis of the Fourth and Fifth Amendments on a historical basis.[88] Subsequent decisions, although criticizing these cases, have not attacked their historical basis.[89]

{47} One possible difficulty with *Boyd*'s argument is that the search and review of papers are themselves the invasion of privacy. That papers that are mere evidence are not then carried away does not eliminate the harm from the search. As Learned Hand wrote, "If the search is permitted at all, perhaps it does not make so much difference what is taken away, since the officers will ordinarily not be interested in what does not incriminate, and there can be no sound policy in protecting what does."[90] However, as Hand continued, "Nevertheless, limitations upon the fruit to be gathered tend to limit the quest itself."[91] In addition, the need for probable cause for a search, coupled with restrictions on what the government may seize, could limit the occurrences of searches of private papers.

{48} Although *Boyd*'s property-oriented approach to the Fourth and Fifth Amendments provides more

support for privacy than the contemporary privacy-based approach of *Katz*,[92] it would be wrong to conclude that the *Boyd* rule would allow unrestricted criminality. Under the *Boyd* line of cases, there could be no Fifth Amendment rights for corporate papers because of the state's visitatorial powers.[93] Under the post-*Boyd* extension of corporate treatment to non-corporate collective entities, organizations such as partnerships, unions, and bankrupt businesses would have no Fifth Amendment protection.[94] If this doctrine covers associations in fact,[95] the scope of communications entitled to Fifth Amendment protection would present few obstacles to law enforcement.

{49} Similarly, *Boyd's* principles allowed the Fourth Amendment seizure of papers sent to another in pursuit of criminality as the instrumentalities of criminal acts.[96] As Justice Marshall observed in dissent, "I see no bar in the Fourth or Fifth Amendment to the seizure of a letter from one conspirator to another directing the recipient to take steps that further the conspiracy.[97]

{50} *Boyd's* definition of Fourth and Fifth Amendment rights would also allow the granting of use immunity to the recipient of a communication to compel the contents of that communication to be used against the sender, or vice versa. An individual may not invoke the Fifth Amendment to protect against incrimination by a third party.[98] Thus, under the Fifth Amendment, encrypted material that one sends to another can be discovered by the government by giving the recipient use immunity for the production of the key, because the Constitution "does not proscribe incriminating statements elicited from another."[99]

B. Implications of the Rejection of *Boyd*

1. Rejection of Precedents

{51} If the Court continues to reject *Boyd*, it will have to reject more than the *Boyd* case. The doctrine that there was substantive protection of documents under the Fourth Amendment and Fifth Amendment, and that an invalid search or seizure under the Fourth Amendment precluded the use of the documents was shared in many opinions, some unanimous and some by the Court's most eminent members. In *United States v. Saline Bank*, Chief Justice Marshall, speaking for the Court, rejected a request for the production of bank documents.[100] "The rule clearly is, that a party is not bound to make any discovery which would expose him to penalties, and this case falls within it."[101] *Hale v. Henkel* affirmed *Boyd*'s holding that "an order for the production of books and papers may constitute an unreasonable search and seizure within the Fourth Amendment."[102] In *Gouled v. United States*,[103] Justice Clarke, speaking for a unanimous court, held when a government agent seized documents in violation of the Fourth Amendment, their introduction into court violated the Fifth Amendent.[104] The Court's *Silverthorne Lumber* opinion by Justice Holmes and Justice Brandeis' famous *Olmstead* dissent are in accord.[105] Many other cases concur.[106]

{52} *Boyd*'s statement has been approved as recently as 1973, when *United States v. Dionisio*[107] stated that the grand jury "cannot require the production by a person of private books and records that would incriminate him."[108] In 1976, even after the *Fisher* decision, the Court wrote in *Andresen v. Maryland*, "'[T]he constitutional privilege against self incrimination . . . is designed to prevent the use of legal process to force from the lips of the accused individual the evidence necessary to convict him or to force him to produce and authenticate any personal documents or effects that might incriminate him.'"[109] *Andresen*, by stating that the government's ability to use information depends on whether it had been produced by subpoena or search, suggests that the government was unable to use subpoenaed documents against their producer.[110] This result would not have followed from a legitimate search under the Fourth Amendment.[111]

{53} The erosion of constitutional protection for private documents proceeded in three ways. First, *Warden v. Hayden* abolished the "mere evidence" rule.[112] Although *Warden*,[113] *Fisher*,[114] and other cases have held out the possibility of protection for diaries, the general rule is that merely evidentiary documents can

now be seized without restriction.[115]

{54} Second, cases have narrowed the scope of evidence that was considered compelled, so that the compelled production of documents was not considered the compulsion of the incriminating evidence in the documents themselves. In *Johnson v. United States*, Justice Holmes wrote for the Court, "A party is privileged from producing the evidence, but not from its production."[116] That phrase led to the idea, in subsequent cases, that compelled production of incriminating information could make the information usable against the person producing it, if that person were screened from the testimonial aspects of production.[117] This interpretation is inapplicable to the facts of *Johnson*, which did not involve an attempt to make a party produce evidence by granting that party limited immunity.[118]

{55} Third, the Court further limited the Fifth Amendment's protection to extend only to testimonial evidence. The origin of this line of authority was cases such as Holmes' opinion in *Holt v. United States,* which held that an accused could be compelled to wear a blouse like that worn by the perpetrator.[119] *Holt*, however, did not distinguish between the act of producing information and the testimonial contents of what was compulsorily produced. Rather, it held that the Fifth Amendment's prohibition only extended to "physical or moral compulsion to extort *communications* from him, not an exclusion of his body as evidence when it may be material."[120] Wearing the blouse was a physical act and not a commnuication. However, the threat of contempt certainly coerces documentary evidence, which is a communication. Thus, *Holt* is entirely consistent with Holmes' opinion for the Court in *Silverthorne Lumber*, which barred a subpoena for documents.[121] *Holt* is also entirely consistent with opinions that Holmes joined such as *Hale,* affirming *Boyd*'s holding that "an order for the production of books and papers may constitute an unreasonable search and seizure within the Fourth Amendment,"[122] and *Gouled,* holding that when a government agent seized documents in violation of the Fourth Amendment, their introduction into court violated the Fifth Amendment.[123]

{56} However, in *Fisher v. United States*, the Court stated that the compulsory production of business documents did not compel testimonial self-incrimination, so it was not prohibited by the Fifth Amendment.[124] The Court reasoned that the author of the statements written in the documents was not compelled to be a witness against himself, because the author had voluntarily written the statements. The Court did hold that any inferences drawn from the act of production itself could be barred.[125] "The elements of compulsion are clearly present, but the more difficult issues are whether the tacit averments of the taxpayer are both 'testimonial' and 'incriminating' for purposes of applying the Fifth Amendment. These questions perhaps do not lend themselves to categorical answers; their resolution may instead depend on the facts and circumstances of particular cases or classes thereof."[126] In that case, the Court concluded that because the papers had been prepared by the accountant and were in the hands of the accountant, their production did not "involve testimonial self-incrimination."[127]

2. Inconsistencies with Other Authority on Privilege

{57} The expansion of other privileges protecting against intrusion into personal thoughts, including work-product immunity, attorney-client and spousal privileges, and self-evaluative privileges, shows that there is no compelling policy reason for rejecting *Boyd*.

{58) Work-product immunity had its origin as a special case of mental privacy, not as a special privilege for attorneys. As the Court wrote in *Hickman v. Taylor*, which invented work-product protection, "[e]xamination into a person's files and records, *including* those resulting from the professional activities of an attorney, must be judged with care. It is not without reason that various *safeguards have been established to preclude unwarranted excursions into the privacy of a man's work*."[128] If the doctrine of mental privacy is to be rejected, then the foundation of *Hickman* and work-product protection is undermined.

{59} Commonly accepted testimonial privileges create at least as much social harm as and have fewer benefits than *Boyd's* protection for private documents.[129] If I write down my daily activities in a letter to an attorney or spouse, keeping a copy for myself, the material is privileged in the hands of the author, the attorney, and the spouse.[130] Both the marital privilege and the *Boyd* privilege for private documents create a zone of autonomy. "From the perspective of the individual in Western industrial societies, the marital relationship is likely to be seen as an extension of one's personal autonomy . . . . It is in this sense that courts often glimpse the relationship between the privilege against self-incrimination and the marital witness privilege."[131]

{60} A diary privilege is even more justified than an attorney-client privilege. Because of the need for legal advice, the attorney-client relationship is less likely to be deterred by a loss of privilege than diary keeping. Moreover, the attorney-client privilege can be used to evade the law[132] or to convey information through a corporation without creating a discoverable paper trail,[133] which weakens the claim for the privilege.

{61} Courts and legislatures have also been creating new privileges. The courts have judicially expanded government privileges, even though the legislature can protect the government. "[G]overnment privileges continue to metastasize."[134] Many jurisdictions have also protected corporate efforts at self-evaluation under the rubric of "self-evaluative privileges." These include general self-evaluative privileges for hospital peer review committees[135] and environmental audits,[136] and other authorities have suggested expanding the privilege in other areas.[137]

{62} Thus, contemporary law generally provides a high degree of privilege for attorneys and those who consult with them, a fair degree of privilege for governments and corporations evaluating themselves, and no privilege at all for those who merely want to write down their ideas. Because the equivalent of the *Boyd* privilege is available to those who have spouses or attorneys and the sophistication to use them in this way, only the shy, the naive, or the single and impoverished need give up their right of privacy.

3. Privacy and Property Rights

{63} In addition to *Boyd*'s consistency with the framers' intent and with other privileges created by a privacy-based approach, its protection of property interests may protect privacy more effectively than tests directly based on privacy.

{64} *Warden v. Hayden*,[138] in which the Supreme Court discerned a "shift in emphasis from property to privacy"[139] in Fourth Amendment rights, significantly eroded protection against governmental searches and seizures. In *Warden v. Hayden*, the Court upheld the seizure of mere evidence, although such a seizure would not have been allowed under property-based interpretations of the Fourth Amendment. In *Katz v. United States*,[140] the Supreme Court followed the *Warden v. Hayden* decision and so resolved the "search" of a telephone conversation by saying that the search invaded privacy, rather than reaching the same result through property law concepts.[141]

{65} This reconstruction of Fourth Amendment law to limit the influence of property law concepts was unnecessary. Justices concurring in the result in *Warden v. Hayden* said so in their opinions.[142] Moreover, *Warden v. Hayden* based the shift to privacy on the argument that common law concepts of property could not explain prior decisions like *Silverthorne Lumber*, which had returned copies of documents illegally seized.[143] However, even before *Warden*, the Supreme Court protected against the unauthorized copying of material, similar to that involved in the *Silverthorne Lumber*.[144] Since *Warden*, the expansion of protection of non-physical property has continued.[145] In *Katz*, the Court protected against electronic eavesdropping; it could have held that a user's payment for a phone call gives him a property interest in the call.[146]

{66} In addition to being unnecessary, the shift in emphasis in Fourth Amendment analysis from property

law to privacy undermined the privacy interests that Justice Brennan, the author of *Warden v. Hayden*, seemed to wish to promote. The undermining arose from the difficulty in defining limits on privacy. No one wanted to protect *every* expectation of privacy-as the Court pointed out, this would provide constitutional protection for the burglar justifiably thinking that his presence in a house would go undiscovered.[147]

{67} To delimit the Fourth Amendment's protection of privacy, the Court in *Rakas v. Illinois* began to confine rights of privacy to those whose expectations of privacy society considered "reasonable." Under *Rakas* and more recent cases following it, "[a] subjective expectation of privacy is legitimate if it is 'one that society is prepared to recognize as "reasonable."'"[148]

{68} However, this made the privacy test circular. How are we to determine that the expectation is "one that society is prepared to recognize as 'reasonable'"?[149] As the *Rakas* Court recognized, "[I]t would, of course, be tautological to fall back on the notion that those expectations of privacy which are legitimate depend primarily on cases deciding exclusionary-rule issues in criminal cases."[150] To avoid this problem, the Court concluded, "Legitimation of expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society."[151]

{69} Despite this recognition in the *Rakas* opinion of the need to avoid tautology, the Court has generally ignored or rejected non-criminal-law sources of an expectation of privacy. The language from the opinion has been used only in *United States v. Jacobsen*, and even in that case, the Court upheld the search.[152] In *Jacobsen*, the Court wrote that "the governmental conduct could reveal nothing about noncontraband items," so that the search was justified.[153] By basing the permissibility of the search on its criminal law consequences, the Court made it more likely that privacy rights would arise only in criminal cases. The Court's restriction of civil claims based on improper searches also reduces the likelihood that a privacy claim would be heard in a non-criminal context.[154]

{70} More recently, the Court has rejected the idea that "concepts of privacy under the laws of each State are to determine the reach of the Fourth Amendment."[155] Thus, even state law recognition of a right to privacy will not make those expectations of privacy reasonable for purposes of the Fourth Amendment.[156] The Supreme Court and state courts frequently differ on what constitutes a reasonable expectation of privacy.[157]

{71} By defining rights of privacy almost exclusively with reference to criminal cases, the Supreme Court has insured that privacy will almost always be pitted against the interest in convicting a criminal. Tying criminal rights to property rights created a general interest in protecting criminals because of the general interest in protecting property rights. Tying criminal rights to property rights also allowed for the expansion of rights against the government as new forms of property arose. Tying criminal rights to a circular test based on "reasonable expectations" that would only be applied in criminal cases served neither of these purposes. Instead, this circularity allowed the Fourth Amendment to be adjusted to the advantage of those in the legal system best able to protect themselves. The very uncertainty of the meaning of the word "privacy" promoted this process.[158] As a result, in several instances a common law expectation of privacy exists because a business interest is involved, but the corresponding interest in privacy under the Fourth Amendment is held to be unreasonable.[159]

IV. Conclusion

{72} Cryptography may provide a technical fix for Supreme Court decisions allowing the invasion of one's private papers. However, the effectiveness of that fix will depend on whether the Court holds that use immunity from the compulsory production of a cryptographic key extends to the incriminating documents

decrypted with the key. Logic suggests that the Court should so hold.

{73} However, the Court's inconsistencies in this area suggest the limits of logic. The Court has consistently reconstructed Fourth and Fifth Amendment precedents to move away from historical practice. This reconstruction is in part responsible for the Court's inconsistencies.

{74} A more sound approach would be to adhere to the usual practice of viewing the Fourth and Fifth Amendments as adopting the practices of the framers at the time of the framing. This would revive broad protection for merely evidentiary materials. Moreover, it would allow constitutional protections to evolve along with social needs, as reflected in society's changing definition of property.

Footnotes

[*]Greg S. Sergienko, 1980. A.B. Harvard College magna cum laude; degree in Social Studies;
1980-1982. Programmer/analyst in computational geometry, computer graphics, and systems programming for Abt Computer Graphics Corp. and Geographic Systems Inc.;
1985. J.D. Harvard Law School magna cum laude;
1985-1986. Law Clerk for the Honorable Alfred T. Goodwin, United States Court of Appeals for the Ninth Circuit;
1986-1993. Associate, Cable Barrett Langenbach & McInerney and Barrett Hale & Gilman;
1993-1994. Bigelow Fellow and Lecturer in Law, University of Chicago Law School;
1994-1996. Visiting Assistant Professor, University of Richmond Law School;
Spring 1995. Adjunct Professor, William & Mary Law School.

[**]**NOTE:** All endnote citations in this article follow the conventions appropriate to the edition of THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION that was in effect at the time of publication. When citing to this article, please use the format required by the Seventeenth Edition of THE BLUEBOOK, provided below for your convenience.

Greg S. Sergienko, *Self Incrimination and Cryptographic Keys*, 2 RICH. J.L. & TECH. 1 (1996), *at* http://www.richmond.edu/jolt/v2i1/sergienko.html.

[1] U.S. CONST. amend. V. The Fifth Amendment's privilege against self incrimination was applied to the states through the Fourteenth Amendment in Malloy v. Hogan, 378 U.S. 1 (1964). This protection means that no government within the federal system can compel testimony that would incriminate the witness in proceedings brought before any other government's courts. Murphy v. Waterfront Comm'n, 378 U.S. 52, 77-78 (1964).

[2] Programs using encryption keys can now make information highly resistant to decrypting even if the algorithm for encrypting the information is known. A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 886 & nn. 767, 768 (1995). For purposes of this paper, the term "cryptographic key" will refer to that without which the government may not gain access to the underlying plaintext. In a public key cryptosystem, this would be the user's private key (and corresponding passphrase); in a private key cryptosystem, this would be the private key. It is conceivable that in other cryptosystems, the "key" could very well be a word or even a phrase.

[3] 387 U.S. 294, 304 (1967).

[4] *Id*.at 303.

[5] *Id*.; Fisher v. United States, 425 U.S. 391, 407 n.9 (1976).

[6] *Compare In re* Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992, 1 F.3d 87 (2d Cir. 1993), *cert. denied,* 114 S. Ct. 920 (1994) (holding that there is no protection for private papers) *with In re* Grand Jury Dubpoena Duces Tecum Dated Oct. 29, 1992, 1 F.3d at 95-96 (concluding that such protection still exists) (Altimari, J., dissenting). Justice O'Connor has declared in a concurring opinion that "the Fifth Amendment provides absolutely no protection for the contents of private papers of any kind." United States v. Doe, 465 U.S. 605, 618 (1984) (Doe I) (O'Connor, J., concurring). Justices Brennan and Marshall expressly disagreed. *Id*. at 619 (Marshall, J., joined by Brennan, J., concurring in part and dissenting in part). Moreover, a post-*Doe* decision stated that the Fifth Amendment privilege reflects "our respect for the inviolability of the human personality and of the right of each individual 'to a . . . private life.'" Pennsylvania v. Muniz, 496 U.S. 582, 595 n.8 (1990) (quoting Doe v. United States, 487 U.S. 201, 212-13 (1988) (Doe II) (quoting Murphy v. Waterfront Comm'n, 378 U.S. 52, 55 (1964) (internal citations omitted))). This statement is difficult to reconcile with interpretations of the Fifth Amendment providing no protection for existing documents.

[7] *Fisher,* 425 U.S. at 409-10.

[8] *Id*. at 401 n.7.

[9] The original message is called the "plaintext." A key is used by a cipher to transmute the plaintext into a ciphertext. Froomkin, *supra* note 2, at 713-14.

[10] *E.g*., Doe v. United States, 487 U.S. 201 (1988) (Doe II) (stating that a directive to disclose bank records was not testimonial).

[11] *Id*. at 210.

[12] *Id*. at 210 n.9 (contrasting "be[ing] forced to surrender a key to a strongbox containing incriminating documents" with "be[ing] compelled to reveal the combination to [petitioner's] wall safe"). Supreme Court Justices have expressed even further doubt as to the meaning of "testimonial." California v. Byers, 402 U.S. 424, 462 (1971) (Black, J., dissenting).

[13] Warden v. Hayden, 387 U.S. 294, 302-03 (1967) ("The items of clothing involved in this case are not 'testimonial' . . . in nature, and their introduction therefore did not compel respondent to become a witness against himself in violation of the Fifth Amendment.") (citing Schmerber v. California, 384 U.S. 757, 761 (1966)).

[14] Schmerber v. California, 384 U.S. 757 (1966).

[15] Pennsylvania v. Muniz, 496 U.S. 582 (1990).

[16] *See, e.g*., MASS. GEN. L. ch. 272, §§ 18 (fornication), 21 (distributing contraceptives) (1992 & Supp. 1995); MASS. GEN. L. ch. 277 § 39 (1992 & Supp. 1995) (defining fornication as "[s]exual intercourse between an unmarried male and an unmarried female"); 18 U.S.C. §§ 707, 711, 711a (1994) (prohibiting the misuse of the 4-H symbols and characters Smokey Bear and Woodsy Owl, respectively).

[17] *See* Gunn v. Hess, 367 S.E.2d 399 (N.C. 1988) (sustaining Fifth Amendment privilege for fear of prosecution for adultery and fornication); Hollowell v. Hollowell, 369 S.E.2d 451 (Va. App. 1988); *In re*

Grant, 264 N.W.2d 586 (Wis. 1978); Choi v. State, 560 A.2d 1108 (Md. 1989) (prosecution's statement that it would not prosecute did not remove privilege).

[18] The possibility of a testimonial key suggests one respect in which use immunity may be broader than transactional immunity. Transactional immunity extends "absolute immunity against future prosecution for the offense to which the question relates." Counselman v. Hitchcock, 142 U.S. 547, 586 (1892). Use immunity, by contrast, requires the prosecution to show that "the evidence it proposes to use is derived from a legitimate source wholly independent of the compelled testimony." Kastigar v. United States, 406 U.S. 441, 460 (1972). "Immunity from the use of compelled testimony, as well as evidence derived directly and indirectly therefrom, affords this protection." *Id*. at 453.
Thus, transactional immunity for the compulsory production of the cryptographic key would extend protection only to the offense mentioned in the testimonial key, not to the wholly unrelated transaction mentioned in the document. In the example in the text, that might be fornication in Massachusetts or using Woodsy Owl to advertise one's 4-H group. Because the plaintext of the document is derived from the key, the protection under use immunity must extend to the wholly unrelated crime mentioned in the document--say, a bank robbery. Whether the Supreme Court in a future case that raises this issue remains true to its verbal formulations is beyond the scope of this paper.

[19] One difference that may be significant as an evidentiary matter, but which will not alter duties to produce the key, is that a cryptographic key that encrypts documents may not be able to decrypt them. Froomkin, *supra* note 2, at 890-94 (describing public-key encryption). By contrast, a safe-deposit box key that locks the box must be capable of opening the box. Public-key encryption means that one cannot assume that the possessor or even the encrypter of encrypted files can decrypt them. Thus, even if the government finds encrypted files in a person's possession, a dishonest possessor may be credibly able to deny the ability to decrypt the documents.

[20] Doe v. United States, 487 U.S. 201, 210 n.9 (1988) (Doe II). The Court had earlier suggested that the privilege could exist with respect to a combination to a safe. Couch v. United States, 409 U.S. 322, 333 & n.16 (1973) (citing United States v. Guterma, 272 F.2d 344 (2d Cir. 1959)).

[21] 8 JOHN H. WIGMORE, EVIDENCE § 2265, at 400 (John T. McNaughton rev., 1961). *See also* MICHAEL J. SAKS &REID HASTIE, SOCIAL PSYCHOLOGY IN COURT (1978).

[22] Schmerber v. California, 384 U.S. 757, 764 (1966) (quoting Counselman v. Hitchcock, 142 U.S. 547, 562 (1892)). *See also* United States v. Cloyd, 25 C.M.R. 908, 914-15 (1958); Heichelbech v. State, 281 N.E.2d 102, 105 (Ind. 1972).

[23] 496 U.S. 582 (1990).

[24] *Id*. at 598-99.

[25] *Id*. at 599.

[26] *Id*. *Cf*. Braswell v. United States, 487 U.S. 99, 126 (1988) (Kennedy, J., dissenting) ("Physical acts will constitute testimony if they probe the state of mind, memory, perception, or cognition of the witness").

[27] Although Counselman v. Hitchcock, 142 U.S. 547, 586 (1892), held that a guarantee of immunity, "to be valid, must afford absolute immunity against future prosecution for the offense to which the questions relates," *Kastigar* held that this "transactional immunity" was unnecessary, so long as the prosecution showed that "the evidence it proposes to use is derived from a legitimate source wholly independent of the compelled testimony." Kastigar v. United States, 406 U.S. 441, 460 (1972). "Immunity from the use of compelled testimony, as well as evidence derived directly and indirectly therefrom, affords this protection." *Id*. at 453.

[28] *Federal Guidelines for Searching and Seizing Computers*, 56 CRIM. L. REP. (BNA) No. 12, at 2023, 2038 (Dec. 21, 1994).

[29] Braswell v. United States, 487 U.S. 99, 118 (1988).

[30] United States v. Doe, 465 U.S. 605, 612-14 (1984) (Doe I).

[31] Froomkin, *supra* note 2, at 872 n.711.

[32] Fisher v. United States, 425 U.S. 391, 410 (1976).

[33] *Doe I,* 465 U.S. at 614 n.13.

[34] *Id*. at 613. Moreover, as the *Fisher* Court observed, because the papers belonged to the accountant, the taxpayers' production of the papers would not serve to authenticate or vouch for the accuracy of the accountant's work. *Fisher*, 425 U.S. at 413. *See also* Braswell v. United States, 487 U.S. 99, 104 n.3 (1988). *Accord In re* Grand Jury Proceedings: Subpoenas for Documents, 41 F.3d 377, 380 (8th Cir. 1994) (barring production, because the government could not independently authenticate the documents and failed to provide use immunity).

[35] *Fisher,* 425 U.S. at 411.

[36] *Braswell*, 487 U.S. at 130 (Kennedy, J., dissenting) (noting that once immunity is granted, the government "would be free to use the contents of the records against everyone, and it would be free to use any testimonial act implicit in production against all but the custodian it selects."). *Cf. Doe I*, 465 U.S. at 617 n.17 (1984) (rejecting the argument that "any grant of use immunity must cover the contents of the documents as well as the act of production", because "use immunity need only protect . . . from the self-incrimination that might accompany the act of producing. . . .").

[37] *Fisher* also cannot and does not purport to represent a holding on the subject of the production of papers written by the person under subpoena. *See Fisher*, 425 U.S. at 394 (the items sought were written by the accountant, with the possible exception of some correspondence that would have been seizable under the *Boyd* case as an instrumentality of fraud).

[38] *See Doe I,* 465 U.S. at 615-16.

[39] *Id*. at 605.

[40] Doe v. United States, 487 U.S. 201 (1988) (Doe II).

[41] Braswell v. United States, 487 U.S. 99, 102 (1988).

[42] Kastigar v. United States, 406 U.S. 441, 460 (1972). The statutes governing use immunity provided by federal law are 18 U.S.C. §§ 6002, 6003 (1994).

[43] *Kastigar*, 406 U.S. at 453.

[44] *Id*. at 460.

[45] *Id*. *Kastigar*, by suggesting that one can use the coerced confession cases to show when the use of evidence derived from compelled statements is impermissible, shows that a causal relationship between the compelled testimony and the evidence sought to be introduced is enough. *See id*. at 461.

[46] *Kastigar*, 406 U.S. at 458-59 (quoting Murphy v. Waterfront Comm'n, 378 U.S. 52, 79 (1964)). Use immunity applies to "the compelled testimony and its fruits." Murphy v. Waterfront Comm'n, 378 U.S. 52, 79 (1964). Under this rule, the prosecutors in a second proceeding "have the burden of showing that their evidence is not tainted by establishing that they had an independent, legitimate source for the disputed evidence." *Id*. at 79 n.18.

[47] That the test is one of cause in fact and not one of the use of the compelled testimony itself seems clear from the Court's use of the "fruit of the poisonous tree" analysis. *See Kastigar*, 406 U.S. at 461. However, the analysis is stricter for compelled testimony. *Id*. If the motive for a witness' testimony is immunized testimony, the testimony of the witness who was motivated by the immunized testimony cannot be used. United States v. North, 920 F.2d 940, 942 & n.1 (D.C. Cir. 1990) (citing United States v. Brimberry, 803 F.2d 908, 915-17 (7th Cir. 1986); United States v. Hampton, 775 F.2d 1479, 1489 (11th Cir. 1985); United States v. Kurzer, 534 F.2d 511, 517-18 (2d Cir. 1976)).

[48] 354 U.S. 118 (1957).

[49] Braswell v. United States, 487 U.S. 99, 114 (1988) (citing *Curcio*, 354 U.S. at 123-24).

[50] Gouled v. United States, 255 U.S. 298, 306 (1921) (Clarke, J., for a unanimous court). *Gouled* expressly held that when a government agent seized documents in violation of the Fourth Amendment, their introduction into court violated the Fifth Amendment. *Id*. *See also*, *e.g*., Olmstead v. United States, 277 U.S. 438, 478-79 (1928) (Brandeis, J., dissenting) ("To protect that right [of privacy], every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And the use, as evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth."); Silverthorne Lumber Co. v. United States, 251 U.S. 385, 391 (1920) (Holmes, J.).

[51] *Gouled,* 255 U.S. at 306.

[52] Braswell v. United States, 487 U.S. 99, 130 (1988) (Kennedy, J., dissenting) (once immunity is granted, the government "would be free to use the contents of the records against everyone, and it would be free to use any testimonial act implicit in production against all but the custodian it selects").

[53] A possible analogy is the compulsory interpretation of documents. My research has turned up no cases involving interpretation. Independently, Froomkin states, "I have been unable to find a single criminal case in which the government has attempted to force a defendant to translate her message." Froomkin, *supra* note 2, at 866 n.687. One civil case upheld a witness' refusal to explain a tape, though he was the only one who could do it. Traficant v. Commissioner, 89 T.C. 501 (1987), *aff'd*, 884 F.2d 258 (6th Cir. 1989). The compulsory production of a cryptographic key is not so invasive in one respect as compulsory interpretation, because there is no judgment involved or continuing cognitive work involved in producing the key: either it works or it does not work.

[54] Doe v. United States, 487 U.S. 201, 210 (1988) (Doe II).

[55] United States v. Euge, 444 U.S. 707, 717 n.11 (1980) (citing United States v. Dionisio, 410 U.S. 1, 6 (1973)).

[56] United States v. Doe, 465 U.S. 605, 611 (1984) (Doe I) (quoting Fisher v. United States, 425 U.S. 391, 409 (1976)).

[57] Counselman v. Hitchcock, 142 U.S. 547, 566 (1892).

[58] *E.g.*, United States v. Sindel, 53 F.3d 874, 876 (8th Cir. 1995) (client identity and fee information not ordinarily privileged, but would be privileged where they would supply the last link in implicating the client or revealing confidential communications); United States v. Sanders, 979 F.2d 87, 91 (7th Cir. 1992); *In re* Grand Jury Proceedings, 946 F.2d 746, 748 (11th Cir. 1991) (concern for own liability); *In re* Grand Jury Proceedings, 906 F.2d 1485, 1491 (10th Cir. 1990) (semble); *In re* Grand Jury Subpoenas, 896 F.2d 1267, 1273 (11th Cir. 1990); *In re* Grand Jury Proceedings, 680 F.2d 1026, 1027 (5th Cir. 1982) (last link test); NLRB v. Harvey, 349 F.2d 900, 905 (4th Cir. 1965) (the identity of the client may be privileged "when so much of the actual communication has already been disclosed that identification of the client amounts to a disclosure of a confidential communication"); State v. Lamb, 690 P.2d 764, 769 (Ariz. 1984) (semble).

[59] *See* Froomkin, *supra* note 2, at 895-97.

[60] *See id.* at 888-89.

[61] Andresen v. Maryland, 427 U.S. 463, 473-74 (1976).

[62] *Id.* at 475 (citing Bellis v. United States, 417 U.S. 85, 88 (1974)).

[63] United States v. Doe, 465 U.S. 605, 614 n.13 (1984) (Doe I).

[64] *Id.* (quoting Fisher v. United States, 425 U.S. 391, 411 (1976)).

[65] 24 CHARLES A. WRIGHT & KENNETH W. GRAHAM, JR., FEDERAL PRACTICE AND PROCEDURE: EVIDENCE § 5484, at 337 & n.140 (1986).

[66] *See* cases cited *supra* note 6.

[67] 493 U.S. 549 (1990).

[68] *In re* Grand Jury Subpoena Duces Tecum Dated October 29, 1992, 1 F.3d 87, 92 (2d Cir. 1993).

[69] *Id.* at 95 (Altimari, J., dissenting).

[70] Hale v. Henkel, 201 U.S. 43, 74-75 (1906). Thus, where privacy is not an issue, as under the Fourth Amendment's protection from searches and seizures and the takings clauses, the corporations have the same rights as individuals. *Id.* at 76.

[71] Pennsylvania v. Muniz, 496 U.S. 582, 595 n.8 (1990) (quoting Doe v. United States, 487 U.S. 201, 212-13 (1988) (quoting Murphy v. Waterfront Comm'n, 378 U.S. 52, 55 (1964) (internal citations omitted))). This language from *Murphy* has also been quoted in other cases. *E.g.*, Couch v. United States, 409 U.S. 322, 328 (1973).

[72] 116 U.S. 616 (1886).

[73] *Id.* at 634-35. Cases after *Boyd* observe that a search for papers that the government seizes by main force was as much a "physical compulsion" as the threat of a contempt sentence for failure to produce. *See, e.g.*, Gouled v. United States, 255 U.S. 298, 305-06 (1921).

[74] *Boyd*, 116 U.S. at 622-30.

[75] *Id.* at 623.

[76] *Id*.

[77] *Id*. at 624.

[78] Gouled v. United States, 255 U.S. 298, 308 (1921) (burglars' tools and weapons).

[79] *Id*. at 309 ("[s]tolen or forged papers" and "contracts . . . used as instruments or agencies for perpetrating frauds.").

[80] *See* Boyd, 116 U.S. at 626-27, 630.

[81] *Id*. at 630.

[82] *Id*. at 630-32.

[83] *Id*. at 622-23.

[84] *Id*. at 629.

[85] *Id*. at 631-32.

[86] *Id*. at 622-23.

[87] *Id*. at 633. *Cf*. BERNARD BAILYN, THE IDEOLOGICAL ORIGINS OF THE AMERICAN REVOLUTION vii-viii (1967) (arguing the influence of British legal precedents on American institutions at the framing).

[88] Gouled v. United States, 255 U.S. 298, 308-09 (1921) (Clarke, J., for a unanimous court).

[89] *E.g*., Fisher v. United States, 425 U.S. 391, 407 (1975) (suggesting only that *Boyd* has "not stood the test of time").

[90] United States v. Poller, 43 F.2d 911, 914 (2d Cir. 1930).

[91] *Id*.

[92] *See* Katz v. United States, 389 U.S. 347 (1967).

[93] *See* Hale v. Henkel, 201 U.S. 43, 74-75 (1906).

[94] *See* Fisher v. United States, 425 U.S. 391, 411-12 (1975); Braswell v. United States, 487 U.S. 99, 112 (1988).

[95] *Cf*. 18 U.S.C. § 1961(4) (1988) (defining "enterprise" in the Racketeer Influenced and Corrupt Organizations Act to include associations in fact that were not legal entities); National Org. for Women, Inc. v. Scheidler, 114 S. Ct. 798, 803-04 (1994) (noting broad definition of "enterprise").

[96] *See* Gouled v. United States, 255 U.S. 298, 309 (1921).

[97] Couch v. United States, 409 U.S. 322, 350 (1973) (Marshall, J., dissenting).

[98] Hale v. Henkel, 201 U.S. 43, 69-70 (1906).

[99] *Couch*, 409 U.S. at 328. This is congruent with the Fourth Amendment, which does not protect

misplaced confidence, and so avoids privacy issues. Hoffa v. United States, 385 U.S. 293, 302 (1966).

[100] United States v. Saline Bank, 26 U.S. (1 Pet.) 100, 104 (1828).

[101] *Id*. The Court rejected Justice Harlan's argument that "*Saline Bank* stands for no constitutional principle whatever." Murphy v. Waterfront Comm'n, 378 U.S. 52, 69 n.11 (1964) (criticizing Hutcheson v. United States, 369 U.S. 599, 608 n.13 (1962) (Harlan, J., plurality opinion) (citing 2 JOSEPH STORY, COMMENTARIES ON EQUITY, § 1494 n.1 (1836))).
Early commentators have likewise concluded that the privilege protects against "the production of *documents* or *chattels* by a person (whether ordinary witness or party witness) in response to a subpoena, or to a motion to order production, or to other form of *process relying on his moral responsibility for truthtelling*." *See* 8 WIGMORE, *supra* note 21, § 2264, at 379 n.1 (emphasis in original). Pennsylvania v. Muniz, 496 U.S. 582 (1990), goes beyond Wigmore by prohibiting the use of information that was not sought for its truth and by suggesting that prohibition extends to the use of physical data as part of a lie-detector test. Wigmore does suggest that the testimonial content is "the witness' assurance, compelled as an incident of the process, that the articles produced are the ones demanded." *Id*. at 380, *cited with approval in* Fisher v. United States, 425 U.S. 391, 411 (1975).

[102] Hale v. Henkel, 201 U.S. 43, 76 (1906). *Accord* Weeks v. United States, 232 U.S. 383, 397 (1914) (quoting *Hale*).

[103] 255 U.S. 298 (1921).

[104] *Id*. at 306.

[105] Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting); Silverthorne Lumber Co. v. United States, 251 U.S. 385, 391 (1920) (Holmes, J.).

[106] *See*, *e.g*., United States v. White, 322 U.S. 694, 698 (1944); Wilson v. United States, 221 U.S. 361, 377 (1911).

[107] 410 U.S. 1 (1973).

[108] *Id*. at 11.

[109] Andresen v. Maryland, 427 U.S. 463, 475 (1976) (citing Bellis v. United States, 417 U.S. 85, 88 (1974) (quoting United States v. White, 322 U.S. 694, 698 (1944))).

[110] *Id*. at 473-74.

[111] *Id*. ("Thus, although the Fifth Amendment may protect an individual from complying with a subpoena for the production of his personal records in his possession because the very act of production may constitute a compulsory authentication of incriminating information, . . . a seizure of the same materials by law enforcement officers differs in a crucial respect, -- the individual against whom the search is directed is not required to aid in the discovery, production, or authentication of incriminating evidence."). *Id*.

[112] Warden v. Hayden, 387 U.S. 294, 301-02 (1967).

[113] *Id*. at 302-03.

[114] Fisher v. United States, 425 U.S. 391, 401 n.7 (1976).

[115] *See* Warden v. Hayden, 387 U.S. 294, 301-02 (1967).

[116] Johnson v. United States, 228 U.S. 457, 458 (1913). Holmes' opinion was quoted by the Court in Couch v. United States, 409 U.S. 322, 328 (1973). *Couch* further suggested that the Fifth Amendment might be violated by "[i]nquisitorial pressure . . . to . . . produce incriminating documents," but there was no such pressure "[i]n the present case." *Id*. at 329.

[117] *See* Andresen v. Maryland, 427 U.S. 463, 473 (1976); *Couch*, 409 U.S. at 328.

[118] *Johnson*, 228 U.S. at 458. The defendant objected to the bankruptcy trustee's producing records that incriminated the bankrupt person. *Id*.

[119] Holt v. United States, 218 U.S. 245, 252-53 (1910) (Holmes, J.).

[120] *Id*. at 252-53 (emphasis added).

[121] Silverthorne Lumber Co. v. United States, 251 U.S. 385, 391 (1920).

[122] Hale v. Henkel, 201 U.S. 43, 76 (1906). *Accord* Weeks v. United States, 232 U.S. 383, 397 (1914).

[123] Gouled v. United States, 255 U.S. 298, 306 (1921).

[124] Fisher v. United States, 425 U.S. 391 (1976).

[125] *Id*.

[126] *Id*.

[127] *Id*. at 411. (The Court's concern for testimonial incrimination may have been dictated by Curcio v. United States, 354 U.S. 118, 125 (1957), which held that because production identified and authenticated a document, further compulsory identification or authentication did not violate the privilege.)

[128] *Id*. at 497 (emphasis added). *See also id*. at 510-511.

[129] The Court has the power to fashion a common-law privilege under Federal Rule of Evidence 501. *Cf*. Trammel v. United States, 445 U.S. 40 (1980) (narrowing common law privilege against adverse spousal testimony). The Court has in the past held that a privilege exists against discovery of material that would expose a party to penalties. United States v. Saline Bank, 26 U.S. (1 Pet.) 100, 104 (1828) (Marshall, C.J.) ("The rule clearly is, that a party is not bound to make any discovery which would expose him to penalties, and this case falls within it."). Of course, a non-constitutional privilege rule would not apply to the states or, in current law, in diversity cases in federal court. FED. R. EVID. 501.

[130] 24 WRIGHT & GRAHAM, *supra* note 65, § 5484, at 324 & n.42 (citing JOHN HENRY WIGMORE, WIGMORE'S CODE OF THE RULES OF EVIDENCE § 2436 (3d ed. 1942)) (attorney); 25 WRIGHT & GRAHAM, *supra* note 65, § 5572, at 473 (spouse).

[131] 5 WRIGHT & GRAHAM, *supra* note 65, § 5572, at 479. See also *id*. at 493 (discussing marital privilege in relation to self-incrimination).

[132] *E.g*., *In re* Grand Jury Proceedings, 600 F.2d 215 (9th Cir. 1979) (shielding fee payments); *In re* Grand Jury Proceedings, 517 F.2d 666, 670-71 & nn. 2-3 (5th Cir. 1975) (semble, collecting cases); Baird v. Koerner, 279 F.2d 623 (9th Cir. 1960) (anonymous restitution to IRS through attorney); Tillotson v.

Boughner, 350 F.2d 663 (7th Cir. 1965) (semble).

[133] Upjohn Corp. v. United States, 449 U.S. 383 (1981). *See* Note, *Privileged Communications: Inroads on the "Control Group" Test in the Corporate Area*, 22 SYR. L. REV. 759, 762 (1971); David Simon, *The Attorney-Client Privilege As Applied to Corporations*, 65 YALE L.J. 953, 955-56 (1956); Note, *Attorney Client Privilege for Corporate Clients: The Control Group Test*, 84 HARV. L. REV. 424, 427 (1970).

[134] 26 WRIGHT & GRAHAM, *supra* note 65, § 5663, at 20 (Supp. 1995).

[135] Bredice v. Doctors Hosp., Inc., 50 F.R.D. 249 (D.D.C. 1970), *aff'd*, 479 F.2d 920 (D.C. Cir. 1973) (protecting minutes of hospital staff meetings regarding improvement in patient care from discovery in a malpractice suit); Health Care Quality Improvement Act of 1986, 42 U.S.C. § 11112(a) (1988).

[136] Fourteen states have environmental audit privilege laws. Those states are: Arkansas, 1995 ARK. ACTS 350; Colorado, COLO. REV. STAT. ANN. § 13-25-126.5 (West 1987 & Supp. 1995); Idaho, IDAHO CODE § 9-802 (1990 & Supp. 1995); Illinois, ILL. ANN. STAT. ch. 415, para. 5/52.2 (Smith-Hurd 1993 & Supp. 1995); Indiana, IND. CODE ANN. § 13-10-3-3 (Burns 1990 & Supp. 1995); Kansas, 1995 Kan. Sess. Laws 204; Kentucky, KY. REV. STAT. ANN. § 224.01-040 (Michie/Bobbs-Merrill 1995); Minnesota, 1995 Minn. Sess. Law Serv. 168 (West); Mississippi, 1995 Miss. Laws 627; Oregon, OR. REV. STAT. § 468.963 (1992 & Supp. 1994); Texas, 1995 Tex. Sess. Law Serv. 219 (Vernon); Utah, UTAH CODE ANN. § 19-7-104 (1995); Virginia, VA. CODE ANN. §10.1-1198 (Michie 1993 & Supp. 1995); and Wyoming, WYO. STAT. § 35-11-1105 (1994 & Supp. 1995).

[137] *See* Note, *The Privilege of Self-Critical Analysis*, 96 HARV. L. REV. 1083 (1983). *But see* University of Pennsylvania v. EEOC, 493 U.S. 182, 189 (1990) (no privilege of "self-critical analysis" to protect routine internal corporate reviews of safety-related matters); Dowling v. American Hawaii Cruises, Inc., 971 F.2d 423, 425-27 (9th Cir. 1992).

[138] 387 U.S. 294 (1967).

[139] 387 U.S. 294, 304 (1967).

[140] 389 U.S. 347, 353 (1967).

[141] *Id*. at 353.

[142] *See Warden*, 387 U.S. at 310 (Fortas, J., joined by Warren, C.J., concurring in the result) (rejecting the "totally unnecessary . . . repudiation of the so-called 'mere evidence' rule").

[143] *Id*. at 305-06 (citing Silverthorne Lumber Co. v. United States, 251 U.S. 385 (1920) (Holmes, J.); Gouled v. United States, 255 U.S. 298, 308-09 (1921)). Moreover, even if there were no protection against the government's seizure of the property, a search might still offend the Fourth Amendment. *See* United States v. Jacobsen, 466 U.S. 109, 122 n.22 (1984).

[144] *See* International News Serv. v. Associated Press, 248 U.S. 215, 240-41 (1918).

[145] *See*, *e.g*., RESTATEMENT (THIRD) OF UNFAIR COMPETITION, at XI (1995) (describing "increase in the commercial and financial significance of intellectual property"); *Id*. § 38 (protecting against appropriation of trade secrets or the commercial value of another's identity); Note, *An Assessment of the Commercial Exploitation Requirement as a Limit on the Right of Publicity*, 96 HARV. L. REV. 1703 (1983); George M. Armstrong, Jr., *The Reification of Celebrity: Persona As Property,* 51 LA. L. REV. 443 (1991); Midler v. Ford Motor Co., 849 F.2d 460, 462-63 (9th Cir. 1988).

[146] *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION, § 43 (1995) (trade secret protection against information gained from "an unauthorized interception of communications"). "A most fundamental human right, that of privacy, is threatened when industrial espionage is condoned or is made profitable." Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476 (1974) (Burger, C.J.).

[147] Rakas v. Illinois, 439 U.S. 128, 143-44 n.12 (1978).

[148] Minnesota v. Olson, 495 U.S. 91, 95-96 (1990) (quoting Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978) (adopting the reasonableness requirement from Justice Harlan's concurring opinion, Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring))).

[149] Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978) (citing Katz v. United States, 389 U.S. at 361 (Harlan, J., concurring)).

[150] *Id*.

[151] *Id*.

[152] United States v. Jacobsen, 466 U.S. 109, 122 n.22 (1984).

[153] *Id*. at 124 n.24.

[154] Harlow v. Fitzgerald, 457 U.S. 800, 818 (1982) (providing immunity from a civil claim "insofar as [defendants'] conduct [did] not violate clearly established statutory or constitutional rights of which a reasonable person would have known").

[155] California v. Greenwood, 486 U.S. 35, 44 (1988) (using privacy, not property arguments, to uphold a search and seizure of garbage, despite the state court's decision that state law created property interests in garbage). Some state courts have subsequently rejected the United States Supreme Court's finding that there is no reasonable expectation of privacy in garbage. State v. Hempele, 576 A.2d 793 (N.J. 1990); State v. Boland, 800 P.2d 1112 (Wash. 1990).

[156] *Cf*. Swift v. Tyson, 41 U.S. (16 Pet.) 1 (1842) (allowing federal courts to ignore state-court rulings on matters of state law), *overruled on other grounds*, Erie R.R. v. Tompkins, 304 U.S. 64 (1938).

[157] *Compare*, *e.g*., Smith v. Maryland, 442 U.S. 735 (1979) (acquisition of telephone numbers dialed with a pen register did not intrude on dialer's expectation of privacy) *with* State v. Hunt, 450 A.2d 952, 955 (N.J. 1982) (contra); People v. Blair, 602 P.2d 738, 746 (Cal. 1979) (contra); Commonwealth v. Beauford, 475 A.2d 783, 791 (Pa. 1984) (contra); People v. Sporleder, 666 P.2d 135 (Colo. 1983) (contra); State v. Gunwall, 720 P.2d 808, 813 (Wash. 1986) (contra); State v. Thompson, 760 P.2d 1162 (Idaho 1988) (contra); Rothman v. State, 779 P.2d 1, 7 (Haw. 1989) (contra); Richardson v. State, 865 S.W.2d 944, 952-53 (Tex. Cr. App. 1993) (en banc) (contra).

[158] Griswold v. Connecticut, 381 U.S. 479, 509 (1965) (Black, J., dissenting) ("'Privacy' is a broad, abstract and ambiguous concept which can easily be shrunken in meaning but which can also, on the other hand, easily be interpreted as a constitutional ban against many things other than searches and seizures.").

[159] *Compare* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476 (1974) (citing with approval E.I. duPont deNemours & Co. v. Christopher, 431 F.2d 1012 (5th Cir. 1970) (holding that overflights are an invasion of trade secrets), *cert. denied*, 400 U.S. 1024 (1971)) *with* California v. Ciraolo, 476 U.S. 207 (1986) (the Fourth Amendment does not bar such overflights) (reversing People v. Ciraolo, 161 Cal. App. 3d 1081, 1090, 208 Cal. Rptr. 93, 98 (1984) ("the area searched was within defendant's curtilage wherein he could reasonably

entertain an expectation of privacy")); Dow Chemical Co. v. United States, 476 U.S. 227, 231-32 (1986) (Burger, C.J.) (allowing overflights under the Fourth Amendment and expressly distinguishing trade secrets issues) *and with* RESTATEMENT (THIRD) OF UNFAIR COMPETITION, § 43 illustration 3 (1995) (trade secret protection against information gained from an overflight). *Compare* Hoffa v. United States, 385 U.S. 293, 302 (1966) (misplaced confidences are not protected by the Fourth Amendment) *and* Smith v. Maryland, 442 U.S. 735, 743-744 (1979) (pen registers are not protected because the phone company knows the number called) *with* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 41 (1995) (giving trade secrets to someone does not permit that person to pass on the trade secrets to another).
