Richmond Journal of Law and Technology

Volume 7 | Issue 4 Article 3

2001

United States v. Hubbell: Encryption and the Discovery of Documents

Greg Sergienko

Volume VII, Issue 4,

Spring 2001

UNITED STATES V. HUBBELL: Encryption and the Discovery of Documents

by: Greg Sergienko(*)

Cite As: Greg Sergienko, United States v. Hubbell: *Encryption and the Discovery of Documents*, 7 RICH. J.L. & TECH. 31 (Spring 2001), *at* http://www.richmond.edu/jolt/v7i4/article1.html.

TABLE OF CONTENTS

I. Introduction

{1}Five years ago, in a contribution to these pages, I suggested that the Supreme Court's oldest precedents and the original intent of the framers of the Constitution precluded the use of evidence produced under a grant of immunity against the producer, even though the material produced included documents that the producer had not been compelled to write. [1] This implied that information concealed with a cryptographic key could not be used in a criminal prosecution against someone from whom the key had been obtained under a grant of immunity. [2]

{2}The issue, however, was doubtful given the tendency of the Court to confine criminal protections and uncontradicted arguments from a dissent in then-recent Supreme Court cases suggesting that the act of producing documents did not confer derivative use immunity as to the contents of the documents. [3] As a result, some thought that the claim of immunity could not be extended to documents produced under a grant of immunity. [4]

{3}Recently Kenneth Starr, the Independent Counsel investigating the "Whitewater" land dealings, sought to use information derived from material produced under a grant of immunity to prosecute Webster Hubbell, the former United States Associate Attorney General and friend of President Clinton. [5] In *United States v. Hubbell*, [6] decided last Term, the United States Supreme Court reached the issue and held that use immunity under the Fifth Amendment to the United States Constitution [7] required protection of the producer of the information from a prosecution based on the information produced. Chief Justice Rehnquist dissented on the basis of the dissenting judge's decision for the Court of Appeals, which also barred the use of the information in the documents. [8] Justice Thomas, joined by Justice Scalia, concurred with the Court's majority opinion, but suggested that interpreting "witness" in the Fifth Amendment according to its original intent requires a broader protection than that required by the Court. [9]

{4}Starr's action, although it did not seek encrypted information, was consistent with the general practice of the federal government in seeking information on computers. [10] Thus, the *Hubbell* decision is important not only for ordinary requests of production, but also for requests of production that require the target of the subpoena to produce a cryptographic key. [11]

{5}This article contains three parts. First, it briefly reviews the *Hubbell* decision, contrasting the decision

with alternative approaches that the Court has now implicitly rejected. Second, it discusses the implications of the majority's opinion for information on computers. [12] In particular, the application of the *Hubbell* decision to encrypted information is likely to lead to several issues not present in applying the decision to tangible documents. This is because encrypted information will have been transmitted often. Multiple transmission creates the possibility of requiring one person to produce evidence against another and the possibility that information will be transmitted in encrypted form between jurisdictions, at least one of which may not recognize the *Hubbell* decision. Interestingly, the choice of public-key encryption has significant implications in both areas. [13]

{6}Finally, it discusses the implications of Justice Thomas' use of original intent. Although the focus of the Thomas opinion is on the definition of "witness," the use of a historical analysis may lead to a considerably broader protection for private documents.

II. The Opinions in *Hubbell*

A. Justice Stevens' Opinion for the Court

{7}Justice Stevens, writing a characteristically thoughtful opinion for the Court, was joined by all the Justices except for Chief Justice Rehnquist.

{8}In the opinion, Justice Stevens began by citing precedent that distinguished testimonial (or communicative) evidence from other evidence. In his view, "the word 'witness' in the constitutional text limits the relevant category of compelled incriminating communications to those that are 'testimonial' in character." Thus, he cited Justice Holmes' opinion in *Holt v. United States* distinguishing "between the use of compulsion to extort communications from a defendant and compelling a person to engage in conduct that may be incriminating." [14] The Court [15] cited its past precedents requiring a criminal suspect to put on a shirt, [16] or to provide a blood sample, [17] a handwriting exemplar, [18] or a recording of his voice. [19] According to the Court, "The act of exhibiting such physical characteristics is not the same as a sworn communication by a witness that relates either express or implied assertions of fact or belief." [20]

{9}The Court then observed that under its precedents, the contents of papers were not privileged. [21] Although the papers themselves were not privileged, the Court acknowledged that under its precedents, production would have a testimonial aspect, by authenticating the documents produced. [22] The Court emphasized that the privilege applied to any link in the chain that was necessary to convict. [23]

{10}In *Hubbell*, the prosecution argued that because it would not have to introduce the documents into evidence against Hubbell, they were not being used in a manner proscribed by the Constitution. [24] However, the Court observed that "the prosecutor needed [Hubbell's] assistance both to identify potential sources of information and to produce those sources." [25] In the Court's view, the reply to the sweeping subpoena was the "functional equivalent of the preparation of an answer to either a detailed written interrogatory or a series of oral questions at a discovery deposition." [26]

{11}Because the preparation of the response required the use of the mind and the responsibility for truth-telling of Mr. Hubbell, the Court rejected the idea that the compulsory response was a mere physical act. [27] The Court chastised the prosecution for arguably switching positions from its concession in the district court that the production of documents had testimonial aspects to contending in the court of appeals and the Supreme Court that the testimonial aspects were insufficient to justify immunity. [28]

{12}In addition, the Court believed that the prosecutor had misread and ignored its precedents, [29] including *Fisher v. United States* [30] and *United States v. Doe*. [31] *Fisher* allowed the prosecution to use documents, prepared by the taxpayer's accountant and held by his attorney against the taxpayer, on the grounds that the

"existence and location of the papers [were] a foregone conclusion." [32] *Doe*, however, limited this rationale, holding that the production of documents in response to a general subpoena has testimonial aspects. [33] Hence, the Court stated that, "whatever the scope of this 'foregone conclusion' rationale, the facts of this case plainly fall outside of it." [34]

{13}Finally, the Court rejected the prosecutor's argument that someone else was required to show a connection between the produced documents and the prosecution. [35] Thus, since the production of the documents was a necessary link in the chain for Hubbell's prosecution, and since the prosecution did not make the necessary showing, Hubbell was entitled to the dismissal of the charges. [36]

B. Chief Justice Rehnquist's Dissenting Opinion

{14}Chief Justice Rehnquist was the sole dissenter. [37] He adopted Judge Williams' dissenting opinion from the court of appeals. [38] In his dissent, Judge Williams stated his belief that the constitutional privilege and the statute conferring use immunity only shielded the witness from the use of any information resulting from his subpoena response "beyond what the prosecutor would receive if the documents appeared in the grand jury room or in his office unsolicited and unmarked, like manna from heaven." [39] Thus, under the Rehnquist view, the sole protection provided by the grant of immunity was immunity as to the source of the documents; if the prosecution could independently authenticate the documents, there would be no protection.

C. Justice Thomas' Concurring Opinion, Joined by Justice Scalia

{15}Justice Thomas, joined by Justice Scalia, joined in the Court's opinion, but wrote separately to suggest that the current reading of "witness" in the Fifth Amendment was too narrow. He felt that the protection provided by the amendment should extend to non-testimonial as well as testimonial information. [40] The implications of this approach are so significant that I will discuss each separately. [41]

III. The Effect of the *Hubbell* Decision

A. The Hubbell Decision's Rejection of Alternative Approaches

{16}The *Hubbell* decision limits prosecutors' use of documentary information produced pursuant to a grant of immunity. With eight members of the Court joining in the decision, and two advocating more protection, it appears unlikely that the decision will be challenged.

{17}Indeed, it may be a sign of the ease with which the Court reached its conclusion that Justice Stevens found it unnecessary to rely on many recent statements in the Court's opinions which supported the *Hubbell* decision. For example, the *Hubbell* opinion did not cite a 1973 decision, which held that the grand jury "cannot require the production by a person of private books and records that would incriminate him." [42] Furthermore, the *Hubbell* Court only cited its decision in *Andresen v. Maryland* [43] in the context of another case and did not quote its language, "'[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.'" [44] By stating that the government's ability to use information depends on whether it had been produced by subpoena or search, *Andresen* suggests that the government may not use subpoenaed documents against their producer. [45] Lastly, the court could have used other opinions [46] such as Justice Stevens' own dissent in *United States v. Doe (Doe I)*. [47]

{18}In the *Hubbell* decision, the Court implicitly rejected a non-textual approach. Prior to the opinion, some scholars had observed that at the time of the framing, one could have a private conversation in an open field.

[48] Therefore, they believed that the guarantees of privacy should be similarly interpreted now. The Court's contrary view, however, is both more narrowly confined to the text of the amendment and more manageable. Although one could have had a private conversation in an open field in 1789, encryption also grants the power to transmit information to more people in ways that appear to be impossible to decrypt. [49] Additionally, modern weapons of mass destruction make the consequences of private conspiracies far worse than was the case in 1789. Under these circumstances, it would be difficult to apply a test based on historical equivalents.

{19}Because the Court's conclusion seems unchallengeable, at least for the present, further discussion of the issues of use immunity for the compelled introduction of documents in American law must be done using the *Hubbell* formula. The decision channels efforts to discover evidence into paths including: (1) the use of search warrants as a substitute for subpoenas; (2) the use of simulated or actual co-conspirators; and (3) the use of foreign governments. The next sections will discuss these issues in turn.

B. The "Foregone Conclusion" Test under Hubbell and Reliance on Search Warrants

{20}The *Hubbell* decision narrows the usefulness of the compelled production of documents. Although the Court acknowledged the possible existence of the "foregone conclusion" doctrine, [50] the Court found that the government knew that the documents existed and knew their location. [51] Thus, the Court's statement that the facts of *Hubbell* "plainly fall outside" the doctrine [52] will surely discourage prosecutors from relying on the doctrine. Indeed, as I suggest below, it is scarcely credible for a prosecutor to resort to a subpoena when the prosecutor can identify the documents clearly enough to obtain a search warrant. [53] Thus, for information contained in unencrypted documents, the logical response of governments is to resort to search warrants, rather than subpoenas. Under the Supreme Court's present jurisprudence, there are few constitutional obstacles to using a warrant, so long as the government can meet the particularity requirement. [54]

{21}In *Warden v. Hayden*, [55] the Court discarded the rule that the power to search and seize depended on the assertion of a superior right to the property seized. [56] Specifically, the Court 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." [57] However, although the Court continued to use language suggesting that there may be some documents not subject to discovery, [58] no recent case has so held, and some Justices have expressed the opinion that no documents may be shielded. [59] Statements by the Court seem to confirm this result, though the statements are in dictum. For example, in a 1976 case, the Court stated,

> 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. [60]

Absent a reconsideration by the Court of this doctrine, the use of a proper search warrant to discover incriminating documents generally infringes no Fourth or Fifth Amendment interest.

{22}With encrypted documents, it may be relatively easy to demonstrate the particularity necessary to use a warrant to seize the document, because the government will only need to identify the media on which the documents might be stored and seize the media. If the key to the documents is located, and is itself unencrypted, it will be trivially easy for the government to decrypt the message. [61]

{23}However, many people who encrypt documents will avoid writing down an unencrypted key. If this is so, then the government will have to obtain a key from someone. Compelling the production of the key from the target will, of course, trigger Fifth Amendment protection. Indeed, the Court repeated the example of *Doe v. United States (Doe II)*, observing that "[t]he assembly of those documents was like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox."[62] Thus, conveying the key has testimonial content.

{24}With respect to encrypted documents, it seems extremely unlikely that the government could satisfy the foregone conclusion test. Strong methods of encryption reduce the likelihood that the documents could be decrypted without a key. [63] Because of this limitation on the "foregone conclusion" doctrine, *Hubbell* seems certain to provide protection for encrypted information when the prosecution seeks the compulsory disclosure of the key. [64] To avoid disclosure of the key, the government will often seek to obtain the key from someone other than the target. This is discussed in the next section.

C. Obtaining Evidence Without Granting Immunity to the Target

1. Compelling Production of the Key Without Granting Immunity

{25}In some instances, one can compel production of the key without granting immunity. This can be true if the individual from whom the key is compelled is not incriminated by the key or holds no Fifth Amendment rights.

{26}The former instance, absence of incrimination, turns on the rule that the Fifth Amendment privilege is personal to the person subject to the compulsion. [65] This rule, although re-iterated recently, [66] has been long-held. For example, in *Hale v. Henkel*, decided in 1906, the Court stated that the privilege "was never intended to permit [a person] to plead the fact that some third person might be incriminated by his testimony, even though he were the agent of such person." [67] Thus, anyone not incriminated by evidence may be compelled to produce it, at least so long as other privileges are not involved. [68] Consequently, if someone becomes a holder of another person's key, the holder can be compelled to produce it.

{27}The second instance, absence of Fifth Amendment rights, turns on the rule that collective entities, such as corporations and unions, have no Fifth Amendment rights. [69] Thus, in *Braswell v. United States*, the Court held that a custodian of corporate records could not avoid a subpoena seeking records from his corporation through asserting his Fifth Amendment privilege against self-incrimination. [70] This was so despite the fact that Mr. Braswell effectively served as the corporation's sole owner and officer. His wife and mother were nominal officers so as to satisfy a Mississippi law requiring corporations to have three directors because he necessarily operated in a representative capacity, under the "collective entity" doctrine, in his duties as custodian. [71]

{28}Under this rule, an individual acting as a corporate agent cannot assert his personal Fifth Amendment rights; similarly, the act of production can only be used against the corporation and not against the custodian. [72] As a consequence of this rule, if a key is used to encrypt both corporate and personal information, it can be compelled from the corporation, perhaps via the same custodian who encrypted personal documents with it. With the key, the government can decrypt all of the documents, even those of the custodian. Although the custodian will have been incriminated, there will be no violation of the Fifth Amendment. Because the result in cases of individuals not incriminated or entities without Fifth Amendment rights is unaffected by the definition of "witness" in the Fifth Amendment; even the potentially broadened protection suggested by Justice Thomas' concurring opinion would not alter these results. [73]

2. Relying on the Misplaced Confidence of the Key-Holder

{29}Neither the Fifth Amendment nor the Fourth Amendment protect misplaced confidence. [74] Thus, neither amendment prohibits the seizure and use of information that is voluntarily transmitted, even if it is transmitted in the mistaken belief that the person to whom the information is directed is not informing the government of the information received. [75]

{30}Because of this, one obvious response from the government to the *Hubbell* decision is to use its own agents to communicate with those suspected of criminal intent or to induce some person who is involved in a conspiracy to provide evidence to the government. Of course, these tactics are nothing new; they are the same methods applied by the government in any conspiracy where the individuals being investigated have not written down incriminating information.

{31}Pretending to be a criminal in order to trap a criminal is an accepted method of law enforcement. [76] Having governmental agents become a part of the conspiracy is not fundamentally different in situations involving encrypted communications, because the governmental agents will necessarily have the plain text of the message that they send or receive. In some respects, the Internet makes it easier for law enforcement. As several articles have noted, it is far easier for law enforcement officials to impersonate children on the Internet than in real life. [77]

{32}Matters are more difficult for the government where it is attempting to get one co-conspirator to turn state's evidence against the other. A number of familiar problems from ordinary cases would apply, such as determining, on the basis of the biased presentations of some possible defendants, which is the least culpable and most credible of the possible defendants to provide evidence against the rest.

{33}An additional problem for the government in securing cooperation as to encrypted evidence turns on the special difficulties of public-key encryption. In public-key encryption, the encrypting key is different from the decrypting key, and someone possessing only the encrypting key cannot decrypt the document.[78]

{34}Public-key encryption has several advantages for legitimate users.[79] Because the public key cannot decrypt the documents, it can be openly transmitted (hence the name "public-key encryption") without jeopardizing the secrecy of the messages encrypted with that key. This is a substantial advantage over other methods of encryption, under which all messages encrypted with a key will be discoverable by one who obtains that key. In addition, public-key encryption creates a basis for message authentication. [80]

{35}A consequence of the availability of public key encryption is that one cannot assume that the possessor or even the encrypter of encrypted files can decrypt them. That creates several hitherto neglected difficulties for law enforcement.

{36}First, even if the government identifies a witness ready to cooperate, [81] that person may not be able to provide a key that will decrypt the documents. A prudent master criminal will give all her subordinates only the public key, which will leave them unable to decrypt the messages sent with that key. [82] Of course, the subordinates might keep unencrypted copies, but that would put them at risk of a search, which under current law could seize all information for use against them. [83] If the subordinates keep copies of the message encrypted with the public key, the master criminal retains the ability to render substantial assistance by providing the government with her private key, which can then decrypt all the messages on her subordinates' computers encoded with the public key. [84]

{37}The ability of a controlling criminal to turn in others, but not the other way around, will confer on the controlling criminal the ability to obtain a reduction in sentence under the federal sentencing guidelines for providing substantial assistance to the government, while leaving lesser criminals unable to do the same to

her.[85]

> [T]he departure tends to benefit those most deeply involved in crime. Minor participants with limited knowledge of the crimes of others often may have no information that authorities do not already possess ... Even among defendants with equal access to useful information, the availability of a substantial assistance departure may hinge primarily on the timing of their arrests and plea bargains. [86]

{38}Only if the subordinates kept copies of transmitted messages encrypted with a different private key (or with some other encryption algorithm) would they be both safe from searches and from the efforts of the master criminal to curry favor with the authorities. The exacerbation of sentencing disparities through public-key encryption is a comparatively minor point, but the ability of a criminal to frustrate the efforts of the government to obtain cooperation is not.

{39}A second difficulty created by the availability of public-key encryption occurs with uncooperative witnesses. Where the government desires cooperation from a witness, a court can grant immunity to a witness and require her cooperation. Because the witness has immunity, the witness no longer has any legitimate ability to refuse to cooperate based on the Fifth Amendment's guarantee against self-incrimination. [87] If the witness refuses at that point to cooperate, the court can ordinarily order the witness jailed until she cooperates. [88]

{40}This approach may be impossible under current standards for the use of civil contempt. "The paradigmatic coercive, civil contempt sanction, as set forth in *Gompers*, involves confining a contemnor indefinitely until he complies with an affirmative command." [89] The permissibility of using indefinite imprisonment depends on the theory that the contemnor "'carries the keys of his prison in his own pocket.'" [90]

{41}Because of public-key encryption, it is no longer possible to assume that someone who possesses encrypted materials has the ability to decrypt them. The person may have encrypted them with a public key, which does not provide the ability to decrypt the documents. Without that ability to decrypt, "the resulting sanction has no coercive effect. '[T]he defendant is furnished no key,'" [91] because the contempt order to decrypt documents asks the impossible. [92]

{42}In such a case, a coercive contempt order is improper. It is, of course, possible that a dishonest possessor may be credibly able to deny the ability to decrypt the documents. [93] So, if the government can show from other evidence strong reason to believe that the person against whom the government seeks a contempt order actually has the power to decrypt a document, an order may be justified despite a claim of incapacity. [94]

{43}The possibility that a witness is lying in denying possession of a private key should be balanced against the possibility that the government and the judge will erroneously conclude that the witness is lying. As the Supreme Court has recently observed, "the contempt power also uniquely is 'liable to abuse.'" [95]

> Unlike most areas of law, where a legislature defines both the sanctionable conduct and the penalty to be imposed, civil contempt proceedings leave the offended judge solely responsible for identifying, prosecuting, adjudicating, and sanctioning the contumacious conduct. Contumacy 'often strikes at the most vulnerable and human qualities of a judge's temperament,' and its fusion of legislative, executive, and judicial powers 'summons forth . . . the prospect of 'the most tyrannical licentiousness . . .' [96]

{44}For these reasons, the Court has extended procedural protections to some contempt proceedings. The exact applicability of these protections to reluctant witness proceedings may be unclear. In discussing non-

cryptographic keys, the Court has suggested that summary proceedings without juries are permissible, [97] but with such keys, the issue of loss of memory of a comparatively complex phrase does not arise.

{45}Of course, if the government can identify the criminal with the private key, contempt is appropriate. However, it may be that the master criminal acts in the United States only through local agents in this country. Thus, an additional alternative to attempts to obtain or compel keys from witnesses in this country is to rely on other countries to obtain or compel keys from witnesses subject to the jurisdiction of those countries. Although other countries' obtaining evidence through inducements appears to be unobjectionable under the Fifth Amendment, their obtaining evidence through coercion raises Fifth Amendment issues.

D. Compulsion by Other Governments

{46}Under the *Hubbell* decision, federal compulsion of a key is prohibited unless the producer of the key is protected against the use of the documents decrypted with the key. In addition, the decision covers attempts by state governments within the United States. The Fifth Amendment's privilege against self-incrimination was applied to the states through the Fourteenth Amendment in *Malloy v. Hogan*. [98] The importance of this rule is that no government within the federal system of the United States can compel testimony that would incriminate the witness in proceedings brought before the courts of any other government in the system. [99]

{47}The issue internationally is less clear. For several reasons, the issues of compulsory production of a key in cross-border cases is more important than with respect to ordinary documents. First, encrypted documents will frequently be transmitted via e-mail across borders. Second, the availability of public-key encryption, in which the sender of an encrypted message may not be able to decrypt it, means that the only person who can decrypt the message sent may be in another country. [100]

{48}Although many other jurisdictions recognize some ability to avoid incriminating oneself, the substantive standards even of countries with traditions similar to the United States may provide less protection. Thus, the European Court of Human Rights recently ruled that the right to remain silent is guaranteed under the European Convention on Human Rights [101] (formerly known as the Convention for the Protection of Human Rights and Fundamental Freedoms). [102] However, in many respects it appears that the European Union law falls short. In a recent decision, the Court of Human Rights declined to interfere with a judgment on self-incrimination grounds, because the announcement that the petitioners' rights had been infringed would suffice. [103] Similarly, Canada has relatively recently implemented its own guarantees, but these may provide less protection than parallel guarantees in the United States. [104]

{49}Perhaps the *Hubbell* decision may influence developments in other countries which have typically had much less time in which to interpret their written constitutional guarantees [105] in a similar direction. However, if other countries continue to have different substantive standards, the use of testimony compelled in other countries in the United States will turn on the applicability of the Fifth Amendment to cross-border transactions.

{50}In *United States v. Balsys*, presenting the case of an action in the United States that might lead to prosecution elsewhere, no Fifth Amendment privilege attaches. [106] In *Balsys*, the Court concluded that the justification for its adoption of the rule that a state of the United States could not compel testimony that could be used in other jurisdictions in the United States was based on the existence of a combined federal-state form of government in the United States. [107]

{51}The Court rejected another rationale of its prior cases. The Court had stated previously that the purpose of the privilege would be unsatisfied if a person could be convicted in federal court with testimony given under a grant of immunity in state court, and convicted in state court with the same testimony given under a grant of immunity in federal court. [108] In *Balsys*, the Court said that this rationale was limited to instances

in which the two governments were working together in "cooperative federalism" in which the Fifth Amendment applied to both jurisdictions. [109] The Court suggested that some forms of cooperation between governments could trigger scrutiny:

> If it could be said that the United States and its allies had enacted substantially similar criminal codes aimed at prosecuting offenses of international character, and if it could be shown that the United States was granting immunity from domestic prosecution for the purpose of obtaining evidence to be delivered to other nations as prosecutors of a crime common to both countries, then an argument could be made that the Fifth Amendment should apply based on fear of foreign prosecution simply because that prosecution was not fairly characterized as distinctly "foreign." [110]

{52}The application of the Fifth Amendment to trials taking place in the United States courts based on compelled testimony in other countries is, with a few exceptions, largely unsettled. The exceptions have to do with either a strong involvement by the United States government, or with claims under the Due Process Clause, instead of only the Self-Incrimination Clause. In the former category is a case holding that the Fifth Amendment applies to a prosecution by the United States government against United States civilians overseas. [111] In the latter category is the long-standing rule that coerced confessions are inadmissible under the due process clause because of doubts as to their reliability. [112] Finally, limitations on personal jurisdiction, [113] which also operate under the due process clause, may prevent other countries from exerting coercive force by obtaining power to affect property outside their jurisdiction. Indeed, if the United States Supreme Court recognizes limitations on "tag" jurisdiction, other countries' ability to derive evidence seizures of individuals transitorily within their presence could conceivably be limited. [114]

{53}In contrast, the Court held in *Johnson v. Eisentrager* [115] that aliens do not have Fifth Amendment rights outside the sovereign territory of the United States. In dictum, *Eisentrager* generally rejected extraterritorial application of the Fifth Amendment. [116] In addition, the Court has adverted to the statutory procedures for granting immunity and evinced a reluctance to bypass them. [117] Moreover, in *Verdugo-Urquidez,* a Fourth Amendment case involving a search by United States narcotics agents in Mexico, the Court ruled that the absence of a search warrant did not violate the Fourth Amendment. [118] However, significant differences exist between the Fourth and Fifth Amendments. As the Court observed in *Verdugo-Urquidez,* the Fourth Amendment applies to a search, rather than to the trial. [119] Also, the Court gives the phrase "the people," a more narrow reach in the Fourth Amendment context than to the Fifth Amendment's reference to a "person." [120]

{54}Under some circumstances, the Court has barred the use of evidence that individuals obtained in violation of their governing rules regardless of whether they violated the rules of the jurisdiction in which the evidence was being used. Before the exclusionary rule was extended to the states in *Mapp v. Ohio*, [121] the Supreme Court relied upon its "supervisory power over the administration of criminal justice in the federal courts" and rejected the "silver platter" doctrine [122] under which federal authorities prosecuted defendants with evidence seized illegally by state authorities. [123] Similarly, the Court used its supervisory powers to enjoin a federal agent from testifying in a state criminal prosecution concerning an illegal search and from turning over to the State evidence that he had illegally seized. [124]

{55}Combined with these precedents on cooperation between jurisdictions within the United States, the Court's statement in *Balsys* expressing uncertainty about the implications of cooperation in obtaining evidence here for a prosecution in another country [125] indicates the possibility that the Fifth Amendment may be triggered in cases involving cooperation between American courts and foreign courts in joint prosecutions. This possibility will exist whether the information is sought in the United States for use elsewhere or sought elsewhere for use in the United States. However, assessing whether compelled testimony has assisted the prosecution is more easily done in the context of a prosecution instead of a grant of immunity

or decision to confine someone for contempt. As a result, there are reasons for expecting the American courts to be somewhat more receptive to Fifth Amendment claims raised in prosecutions in the United States, supposedly based on evidence compelled elsewhere, than to such claims raised in decisions on compelling testimony in the United States.

E. Independent Discovery

{56}The Court's opinion left undecided one important issue, the extent to which the prosecutor must show the possibility of independent discovery. Under the court of appeals' decision in *Hubbell,* the prosecutor had the burden of "demonstrating with reasonable particularity a prior awareness that the exhaustive litany of documents sought in the subpoena existed and were in Hubbell's possession." [126] On remand, the prosecutor conceded that he could not demonstrate the independence under the court of appeals' standard, and the Supreme Court therefore did not have to address the issue of what showing would be sufficient. [127]

{57}The "reasonable particularity" standard appears to be drawn from the standard for a warrant. [128] The interests involved in immunity are of an entirely different order. Indeed, the "reasonable particularity" standard appears to be a considerably more lenient standard than those used in other cases. Thus, in *United States v. North,* [129] the court required the prosecutor to demonstrate in detail an independent ability to produce the evidence, including demonstrating that the witnesses' testimony was uninfluenced by the compelled evidence, and suggested that the prosecutor could show this by "canning" the witnesses' testimony. [130]

{58}The court of appeals in *Hubbell* did little to explain its decision, beyond citing *Terry v. Ohio* and other Fourth Amendment cases. [131] However, Fourth Amendment cases are inapplicable for several reasons. First, the Fourth Amendment, as the Court has observed in another context, protects an interest that is violated by the search, "and a violation of the Amendment is 'fully accomplished' at the time of an unreasonable governmental intrusion." [132] By contrast, "the privilege against self-incrimination guaranteed by the Fifth Amendment is a fundamental trial right of criminal defendants. Although conduct by law enforcement officials prior to trial may ultimately impair that right, *a constitutional violation occurs only at trial*." [133] The continued use at trial of evidence acquired in violation of the Fifth Amendment is therefore a direct violation of its terms, rather than a consequential injury, as is the case with the Fourth Amendment.

{59}Second, the standard for inevitable discovery as an exception to the exclusionary rule differs from the standard for compelled production under the Fifth Amendment. The inevitable discovery doctrine involves balancing the marginal increase in deterrence resulting from the exclusionary rule against the costs. [134] Because of the deterrence rationale of the rule, attenuation analysis is a way of identifying whether the cost of excluding the evidence to the truth-finding process is worth the benefit to deterring police wrongdoing. [135] Compelled self-incrimination under the Fifth Amendment does not rest on a deterrence rationale. Indeed, the claim may be stronger for the compulsory surrender of the self- incrimination privilege in judicial proceedings than in extra-legal police beatings in Fifth Amendment cases. [136]

{60}It would seem from the Court's analysis that the proper approach is to rely on the "foregone conclusion" approach. As the *Hubbell* decision in the Court of Appeals suggested, only such an approach is consistent with the usual rules on compelled testimony. [137] In such cases, as *Kastigar* held, the prosecution bears the "heavy burden" of establishing an independent source. [138] *Fisher* involved summonses seeking production of working papers prepared by the taxpayers' accountants that the IRS knew were in the possession of the taxpayers' attorneys, [139] and its casual reference to a foregone conclusion should not be taken as exhausting requirements of the rule.

IV. The Implications of the Thomas Opinion

{61}Justice Thomas, joined by Justice Scalia, joined in the Court's opinion, but wrote separately to suggest that the current reading of "witness" in the Fifth Amendment was too narrow, so that the protection provided by the amendment should extend to non-testimonial as well as testimonial information. [140] In the analysis provided by Justice Thomas, the protection of the amendment might reach any evidence, [141] and, in any case, providing evidence pursuant to a subpoena duces tecum was as important as providing in-court testimony pursuant to a subpoena ad testificandum. [142] Under this analysis, the opinion in *Fisher v. United States* [143] is too narrow, [144] although a broader construction of its conclusion to make it consistent with the Thomas approach is possible. [145]

{62}A similar approach was suggested in Justice Black's dissent in *Schmerber v. California*. [146] In that case, the incriminating evidence was a blood sample involuntarily drawn from the defendant, and the Court construed the Fifth Amendment to apply only to "testimonial" conduct. [147] As Justice Black observed in dissent, this interpretation imported a requirement of testimoniality into a Fifth Amendment that does not contain one. [148]

{63}However, it is not clear that the Thomas-Scalia view extends to Justice Black's reasoning in *Schmerber*. On the one hand, Justice Thomas states, "A review of that period reveals substantial support for the view that the term 'witness' meant a person who gives or furnishes evidence, a broader meaning than that which our case law currently ascribes to the term." [149] He buttresses this conclusion by citing dictionaries from "around the time of the founding [that] included definitions of the term 'witness' as a person who gives or furnishes evidence." [150] "Furnishing evidence" would encompass providing blood samples or other physical evidence. It could also encompass appearing in court so that another witness could make an identification.

{64}On the other hand, all the examples that Justice Thomas cites involve testimony or documentary evidence in one form or another, not physical evidence. [151] Moreover, at one point he states that his possible conclusion is only that "[t]he 18th century common-law privilege against self-incrimination protected against the compelled production of incriminating physical evidence such as papers and documents." [152] In addition, he criticizes the Court's prior decision in *Fisher v. United States,* [153] which dealt with documentary evidence, but not *Schmerber v. California*," [154] which dealt with physical evidence. Finally, the difference between physical evidence and communications has long been established. Even when the Court barred searches for documentary evidence, [155] opinions such as *Holt v. United States* confined the protection to communications. [156] *Holt* permitted compelling defendants to wear articles of clothing for identification in court. [157]

{65}The extension of protection to non-documentary evidence would involve a radical change in criminal procedure. Most notably, the extraction of DNA evidence would appear to be prohibited. A constitutional guarantee may not be eliminated merely because it leads to difficult results in particular cases, but the Court might be unsympathetic to a rule that would do away with some of the most reliable evidence available in criminal cases. ln fairness to Justice Thomas, it should be observed that he (and Justice Scalia) only indicated their willingness to reconsider the self-incrimination clause in a future case. [158]

{66}However the Court and Justice Thomas may resolve the uncertainty between verbally incriminating evidence and other evidence, protection of verbally incriminating evidence would be a powerful addition to the Court's current Fifth Amendment protection. Under Thomas's view, a producer of documents would be immune from their use against him, even if the prosecution could otherwise identify the documents, because the person producing the documents would no longer have to show that the production was testimonial.

{67}Even if the original understanding of the Fifth Amendment were sufficiently indeterminate so as not to require such an approach, practicality provides additional support. Under the court of appeals opinion, the prosecutor can use documentary evidence by showing "with reasonable particularity a prior awareness [of]

the ... documents sought in the subpoena existed and [that they] were in [the producer's] possession." [159]

{68}A prosecutor's claim to have been able to establish the documents' location and existence with particularity is suspicious when the prosecutor used a subpoena duces tecum. If the prosecutor had been able to establish the documents' location and existence, the prosecutor would be entitled to a search warrant. [160] A search warrant has the advantage, from the prosecutor's perspective, of not giving the possible defendant notice of the documents and thereby allowing the person subject to the subpoena to destroy the documents. [161] The use of a subpoena duces tecum under such circumstances seems more consistent with an unscrupulous prosecutor's desire to get the documents and then construct an after-the- fact claim to have been able to identify them. (Of course, if the documents were not expected to incriminate the person subject to the subpoena, the prosecutor might not have been deterred by the prospect of expected destruction, and might have favored a subpoena as reducing the workload for the prosecutor and the burden on the person that was a target of the subpoena.)

{69}Although this argument is perhaps most obvious with respect to ordinary documents, the same possibility exists with perhaps even greater force in the instance of encrypted documents. There, the location of the documents on a computer in the custody of the target may be more obvious than the location of voluminous papers. The only practical problem is decrypting the documents. Because the documents will be subject to brute-force decryption, [162] it will be possible for a prosecutor to claim that he had the resources necessary to decrypt a document.

{70}The Thomas view by itself does not provide protection against seizure of documents. Under the most recent Supreme Court precedents,

> [A]lthough 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. [163]

{71}These standards are inconsistent with the opinion at the time of its framing. As the Court observed in *Boyd v. United States*, [164] decided in 1886, the protection against the government's ability to obtain incriminating documentary evidence was the same under the Fourth and Fifth Amendments. [165] Since then, the "mere evidence" rule has been overturned in *Warden v. Hayden*. [166]

{72}The historical analysis that the Court in *Boyd* performed, established the soundness of broader protection for documentary evidence. [167] It is to be hoped that Thomas' opinion, by embarking on a mode of analysis similar to that of *Boyd*, is the first step in the Court's return to a more historically sound view of the Fourth and Fifth Amendments.

V. Conclusion

{73}The government has broad investigatory powers, which allow an intrusion into privacy with little or no justification. A grand jury may inquire into anything with little or no reason and may ask questions without demonstrating their relevance to any inquiry. [168] The FBI has the power to intercept considerable information about individuals through the interception of their e-mails through the so-called "Carnivore" project. [169] Although the FBI maintains that the information it receives is strictly limited, [170] many are skeptical. [171]

{74}With respect to individuals, the *Hubbell* decision and the availability of strong cryptography merely

restore the effect of the law pre-existing the decision in *Warden v. Hayden,* which allowed the government to seize diaries and other "mere evidence," and *Fisher,* which contained dicta seemingly embracing the idea that individuals could be compelled to provide evidence against themselves. [172] Before those decisions, one could record one's confessions in one's diary, confident that the Fifth Amendment barred the government from requiring their production and that the Fourth Amendment prevented their seizure. Because the *Hubbell* decision has restored a long-accepted situation, the dismay of individuals connected with law enforcement at the prospect of not being able to seize diaries and the equivalent seem to be overstated. [173]

{75}With respect to broader conspiracies, the claims of the government may have more merit. The effect of broad protection for cryptography is to conceal a substantial amount of information from the government. Even in such a case, the government is little, if any, worse off than it would be if co- conspirators made no record of their activities and took care not to communicate in ways that could be subject to interception. Because the determinedly guilty have always had ways to shield themselves, the primary effect of encryption is more to assure individuals that their privacy will be respected. As a result of the government's opportunity to obtain information, protecting the vast majority of innocent individuals in their expectations of privacy may require protecting criminals.

ENDNOTES

[*] Associate Professor of Law, Western State University College of Law. The author would like to acknowledge the assistance of Ron Bacigal, Kris Miccio, Brent Romney, and Marcia Wilbur.

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

[2] *See id*.

[3] *See id*. ¶ 21 (citing Braswell v. United States, 487 U.S. 99 (1988) (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."); United States v. Doe, 465 U.S. 605, 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 of immunity need only protect . . . from the self-incrimination that might accompany the act of producing. . . .")).

[4] *See*, *e.g.*, Phillip R. Reitinger, *Compelled Production of Plaintext and Keys*, 1996 U. Chi. Legal Forum 171; D. Forest Wolfe, Comment, *The Government's Right to Read: Maintaining State Access to Digital Data in the Age of Impenetrable Encryption*, 49 EMORY L.J. 711 (2000). Mr. Reitinger was, at the time of his article's publication, a trial attorney with the Computer Crime and Intellectual Property Section, Criminal Division, Department of Justice. 1996 U. CHI. LEGAL FORUM 171 n.*.

[5] *See*, *e.g.*, Bill Miller, *Hubbell Tax Case Challenged by Judge*, WASH. POST, June 27, 1998, at A3.

[6] United States v. Hubbell, 530 U.S. 27 (2000).

[7] The Fifth Amendment provides that no person "shall be compelled in any criminal case to be a witness against himself. U.S. CONST. amend. V.

[8] 530 U.S. at 49 (Rehnquist, C.J., dissenting).

[9] *Id*. (Thomas, J., concurring). The Thomas and Scalia opinion is similar to, although less developed than, the analysis in the earlier article. *See* Sergienko, *supra* note 2, at ¶¶ 40-71.

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

[11] Indeed, because the government is likely to have far more success in using a search warrant to obtain tangible documents than to obtain information encrypted with a reasonably strong program, *Hubbell* is likely to have far more effect with encrypted information than with ordinary documents. *See infra* Part III.B & n.63.

[12] Because the Court's opinion is similar to the analysis suggested in my earlier article, this article will not repeat the full historical analysis in that article. *See* Sergienko *supra* note 2, at ¶¶ 18-28.

[13] A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA . L. REV. 709, 890 (1995), *available at* http://www-swiss.ai.mit.edu/6095/articles/froomkin-metaphor/appendices.html#ToC84.

[14] United States v. Hubbell, 530 U.S. 27, 34 (2000) (construing Holt v. United States, 218 U.S. 245 (1910)).

[15] *Id*. at 35 (construing United States v. Wade, 388 U.S. 218 (1967)).

[16] *Id*. (construing Holt v. United States, 218 U.S. 245 (1910)).

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

[18] Gilbert v. California, 388 U.S. 263 (1967).

[19] United States v. Wade, 388 U.S. 218 (1967).

[20] *Id*. at 35 (citing Pennsylvania v. Muniz, 496 U.S. 582 (1990)).

[21] *Id*.

[22] *Id*.

[23] *Id*.

[24] *Id*. at 39.

[25] *Id*.

[26] *Id*.

[27] *Id*.; *see also id*. at n.23 (citing William J. Stuntz, *Self-Incrimination and Excuse*, 88 COLUM. L. REV. 1227, 1228-29, 1256-59, 1277-79 (1988) (discussing the conceptual link between truth-telling and the privilege in the document production context); Samuel A. Alito, Jr., *Documents and the Privilege Against Self-Incrimination*, 48 U. PITT. L. REV. 27, 47 (1986); 8 John Henry Wigmore, Evidence § 2264, p. 379 (J. McNaughton rev. 1961) (describing a subpoena duces tecum as "process relying on [the witness'] moral responsibility for [*sic*] truthtelling")).

[28] United States v. Hubbell, 530 U.S. 27, 43 (2000).

[29] *Id*.

[30] 425 U.S. 391 (1976).

[31] 465 U.S. 605 (1984).

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

[33] 465 U.S. at 612-14.

[34] United States v. Hubbell, 530 U.S. 27, 44 (2000).

[35] *Id*. (citing Brief for the United States).

[36] *Id*.

[37] *Id*. at 49 (Rehnquist, C.J., dissenting).

[38] *Id*. (citing United States v. Hubbell, 167 F.3d 552 (D.C. Cir. 1999) (Williams, J., dissenting)).

[39] United States v. Hubbell, 167 F.3d 552, 602 (D.C. Cir. 1999) (Williams, J., dissenting) (citing Department of Justice Amicus Brief and Samuel A. Alito, Jr., *Documents and the Privilege Against Self-Incrimination*, 48 U. PITT. L. REV. 27 (1986)).

[40] United States v. Hubbell, 530 U.S. 27, 50 (2000) (Thomas, J., concurring).

[41] *See infra* Part V.

[42] United States v. Dionisio, 410 U.S. 1, 11 (1973) (citing Boyd v. United States, 116 U.S. 616 (1886)).

[43] 427 U.S. 463 (1976).

[44] *Id*. at 475 (citing Bellis v. United States, 417 U.S. 85 (1974) (quoting United States v. White, 322 U.S. 694 (1944)).

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

[46] *See*, *e.g*., *Schmerber*, 384 U.S. at 763-74 ("It is clear that the protection of the privilege reaches an accused's communications, whatever form they might take, and the compulsion of responses which are also communications, for example, compliance with a subpoena to produce one's papers.") (citing Boyd v. United States, 116 U.S. 616 91886)).

[47] 465 U.S. 605 (1984) (hereinafter Doe I). *Compare Hubbell*, 530 U.S. at 43 (under the subpoena, "[i]t was unquestionably necessary for respondent to make extensive use of 'the contents of his own mind') (citing Curcio v. United States, 354 U.S. 118 (1957) and Doe v. United States, 487 U.S. 201 (1988) (hereinafter Doe II) *with Doe II*, 487 U.S., at 219 (Stevens, J., dissenting) ("The expression of the contents of an individual's mind falls squarely within the protection of the Fifth Amendment.") (citing Boyd, 116 U.S. 616 (1886) and Fisher v. United States, 425 U.S. 391 (1976)).

[48] Froomkin, *supra* note 13, at 798.

[49] Authors differ on the availability of secure encryption at the time of the framing. *Compare* Froomkin, supra note 14, at 798-99 (secure encryption available) *and* John A. Fraser, III, *The Use of Encrypted, Coded*

And Secret Communications Is an "Ancient Liberty" Protected by the United States Constitution, 2 VA. J.L. & TECH. 2 (1997) *with* Wolfe, *supra* note 4, at 712 & n.8 (secure encryption not available).

[50] *Hubbell*, 530 U.S. at 44.

[51] *Id*. at 44.

[52] *Id*.

[53] *See infra* Part V.

[54] *See*, *e.g*., Marron v. United States, 275 U.S. 196 (1927) (setting out the particularity standard for a search warrant); Steele v. United States, 267 U.S. 498, 503 (1925) (describing the parameters of the particularity requirement with respect to a building search).

[55] 387 U.S. 294 (1967).

[56] *Id*. at 304.

[57] *Id*. at 303.

[58] *See*, *e.g*., Pennsylvania v. Muniz, 496 U.S. 582, 595 n.8 (1990) (citing Doe II, 487 U.S. 201, 212-13 (1988) (quoting Murphy v. Waterfront Comm'n of New York Harbor, 378 U.S. 52 (1964) (describing "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'") (internal citations omitted))).

[59] 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." *Doe I*, 465 U.S. 605, 618 (1984) (O'Connor, J., concurring). Justices Brennan and Marshall expressly disagreed that *Doe I* addressed the issue. *Id*. at 619 (Marshall, J., joined by Brennan, J., concurring in part and dissenting in part). Because Justice O'Connor joined in the Court's opinion in *Hubbell,* it appears that her *Doe I* concurrence applied only to documents that did not have limitations placed on their use pursuant to compulsory production.

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

[61] Identifying the computer that performed the encryption might somewhat ease the task of decrypting a message. *See* Froomkin, *supra* note 13.

[62] 530 U.S. 27, 43 (2000) (citing Doe, 487 U.S. at 210 n.9). This suggestion of *Hubbell* and *Doe* is consistent with earlier statements by the Court. *See also* Couch v. United States, 409 U.S. 322, 333 & 334 n.16 (1973) (citing United States v. Guterma, 272 F.2d 344 (2d Cir. 1959)); Sergienko, *supra* note 1, at ¶ 12 & n.1.

[63] *See* Sergienko, *supra* note 1, at ¶ 2 & n.2.

[64] It was also possible to arrange for a key to have testimonial and incriminating content. *See* Sergienko, *supra* note 1, at ¶ 9 & nn.16-18.

[65] 201 U.S. 43 (1906).

[66] *See e.g*., Braswell v. United States, 487 U.S. 99 (1988).

[67] *Hale*, 201 U.S. at 69-70. *Hale* suggests that the Fifth Amendment's guarantees apply to the states. *Id*. at 74.

[68] *See* Fisher v. United States, 425 U.S. 391, 396 (1976) (holding that a taxpayer who would have had a Fifth Amendment privilege in the documents will be protected from a subpoena compelling his attorney, to whom the documents had been given for the purpose of obtaining legal advice, from producing them).

[69] *E.g*., Bellis v. United States, 417 U.S. 85 (1974); Braswell v. United States, 487 U.S. 99 (1988).

[70] *Braswell*, 487 U.S. 99, 100 (1988).

[71] *Id*. at 110.

[72] *See id*. at 118 & n.11.

[73] *See infra* Part V.

[74] Hoffa v. United States, 385 U.S. 293, 302-303 (1966). Of course, entrapment is prohibited. *See* Matthews v. United States, 485 U.S. 58 (1988) (allowing entrapment instruction, even if the defendant denies some elements of the crime); Hampton v. United States, 425 U.S. 484 (1976) (denying defense based on due process clause).

[75] Lopez v. United States, 373 U.S. 427 (1963) (governmental agent); On Lee v. United States, 343 U.S. 747 (1952) (non-governmental witness); Hoffa v. United States, 385 U.S. 293 (1966).

[76] Lewis v. United States, 385 U.S. 296 (1966).

[77] Bill Leukhardt, *Policing the Net for Pedophiles*, HARTFORD COURANT, May 6, 2000, at B1 (discussing a course in impersonating children to catch pedophiles); Catherine Edwards, *Pedophiles Prowl the Internet*, WASH. TIMES (D.C.), Feb. 28, 2000, at 14 (citizen activist impersonating children); Gregory Alan Gross, *New Unit Targets Online Molesters*, SAN DIEGO UNION & TRIB., July 9, 2000, at B1; Amy Joi Bryson, *Police Surf Internet to Snag Pedophiles*, DESERET NEWS, Nov. 16, 1999, at B7. *But see* Jacobson v. United States, 503 U.S. 540 (1992) (finding entrapment in repeated attempts at soliciting the purchase of child pornography through the mails).

[78] William A. Hodkowski, Comment, *The Future of Internet Security: How New Technologies Will Shape the Internet and Affect the Law*, 13 SANTA CLARA COMPUTER & HIGH TECH L.J. 217 (1997); Froomkin, *supra* note 13 (explaining public-key encryption).

[79] It has a comparatively trivial disadvantage. For technical reasons, public keys are often longer than private keys, so encoding with public keys takes longer, by a factor of 100 to 10,000, depending on the implementation. Hodlowski, *supra* note 78, at 232-33. In some contexts, this disadvantage can be overcome by using public key encryption to encrypt an equally secure key to another form of encryption, and then exchange information with that other key. *Id*. at 233.

[80] Hodlowski, *supra* note 78, at 233.

[81] "Cooperation" here covers the actions of any person genuinely seeking to assist the government, whether for a reduction in sentence for substantial assistance, or for some other seemingly coercive reason. *See* Federal Sentencing Guidelines, 18 U.S.C.S. App. § 5K1.1 (7) (2000) (citing United States v. Dixon, 998 F.2d 228 (4th Cir. 1993)).

[82] Of course, to receive encrypted messages from the master criminal, the subordinate criminal must have the private key. However, messages going from the master to the subordinate criminal need not have the same key as messages going from the subordinate to the master criminal. And, if prompt delivery is unimportant, the master criminal could simply snail mail encrypted messages, relying on the anonymity of mailing to conceal her identity for transmissions in that direction.

[83] *See supra* note 55.

[84] For the importance of substantial assistance in a sentencing situation, *see* Federal Sentencing Guidelines, 18 U.S.C.S. App. § 5K1.1 (7) (2000) .

[85] *See* Gerald F. Uelmen, *Federal Sentencing Guidelines: A Cure Worse Than the Disease*, 29 AM. CRIM. L. REV. 899, 900-02 (1992). *See also* Federal Sentencing Guidelines, 18 U.S.C.S. § 5K1.1(7) (2000) (defendant's substantial assistance to authorities is valid reason to depart from the Guidelines).

[86] Gerald W. Heaney, *The Reality of Guidelines Sentencing: No End to Disparity*, 28 AM. CRIM. L. REV. 161, 199 (1991) (footnotes omitted). The author was a Senior Circuit Judge, United States Court of Appeals for the Eighth Circuit. *Id*. at 161 n.a.

[87] *E.g*., Murphy v. Waterfront Comm'n of New York Harbor, 378 U.S. 52 (1964).

[88] *Id*.

[89] United Mine Workers v. Bagwell, 512 U.S. 821, 828 (1994) (citing Gompers v. Buck's Stove & Range Co., 221 U.S. 418 (1911)).

[90] *Id*. at 828 (quoting Gompers, 221 U.S. at 442 (quoting In re Nevitt, 117 F. 448 (8th Cir. 1902))).

[91] *Id*. at 829 (quoting Gompers, 221 U.S. at 442).

[92] A witness may also claim simply to have forgotten a key, but that is less plausible with recent transmission of information.

[93] Sergienko, *supra* note 1, at ¶ 19.

[94] One item of evidence might be intercepted Internet transmissions showing that the person from whom information was sought was the recipient of the transmissions. Being a recipient is not readily consistent with possessing only the public key, because only a person with the private key could decrypt the document.

[95] United Mine Workers v. Bagwell, 512 U.S. 821, 831 (1994) (quoting Bloom, 391 U.S. at 202 (quoting Ex parte Terry, 128 U.S. 289, 313 (1888))).

[96] *Id*. at 831 (quoting Bloom, 391 U.S. at 202; Young v. United States ex rel. Vuitton et Fils S.A., 481 U.S. 787, 822 (1987)) (Scalia, J., concurring in judgment) (quoting Anderson v. Dunn, 6 Wheat. 204, 228 (1821)).

[97] *Id*. at 832-33.

[98] Malloy v. Hogan 378 U.S. 1, 6 (1964).

[99] Murphy v. Waterfront Comm'n of New York Harbor, 378 U.S. 52, 77-78 (1964); Kastigar v. United States, 406 U.S. 441, 444-45 (1972).

[100] *See supra* ¶45.

[101] Nov. 4, 1950, art. 6(1), 213 U.N.T.S. 222, 228.

[102] *See* Funke v. France, 256 Eur. Ct. H.R. (ser. A) at 8 (1993) (holding that Article 6(1) of the European Convention on Human Rights guarantees the right against self-incrimination); Ying H. Tan, *Use of DTI Interviews Unfair*, Independent (London), Sept. 30, 1994, at 30 (reporting the decision of the European Commission of Human Rights in Saunders v. United Kingdom).

[103] Frances Gibb, *European Court Backs Guinness Trio*, Times (London), Sept. 20, 2000, at 25 (referring to IJL v. United Kingdom, (unreported, September 19, 2000) (Eur. Ct. Human Rights), *available at* http://www.echr.coe.int/).

[104] "The right not to be compelled to testify against oneself is specifically protected by [Canadian Charter of Rights and Freedoms] § 11(c); the general principle against self-incrimination resides in § 7." R. v. D. (A.S.), 2000 Sup. Ct. Can. 46, 54 (2000).

[105] *See* Mirjan Damaska, *Evidentiary Barriers to Conviction and Two Models of Criminal Procedure*, 121 U. PA. L. REV. 506, 526-30 (1973) (comparing traditional European rules against self-incrimination with American rules).

[106] United States v. Balsys, 524 U.S. 666, 692 (1998).

[107] In an article written shortly before the Court's decision, Diane Marie Amann argued that the problems of two jurisdictions, each compelling testimony to be used in criminal trials, cited by the Court as a reason for applying the self-incrimination clause to bar the use , applied just as much in the international context. *A Whipsaw Cuts Both Ways: The Privilege Against Self- Incrimination in an International Context*, 45 UCLA L. REV . 1201 (1998). The Court expressly rejected this analysis. *Balsys*, 524 U.S. at 695 n.16.

[108] *Balsys*, 524 U.S. at 681-82 (quoting Murphy v. Waterfront Comm'n of New York Harbor, 378 U.S. 52, 55, 79 (1964)).

[109] *Id*. at 694-95 (quoting *Murphy*, 378 U.S. at 55).

[110] *Id*. at 698.

[111] Reid v. Covert, 354 U.S. 1, 5-6 (1957) (plurality opinion); *id*. at 41-42 (Frankfurter, J., concurring).

[112] Brown v. Mississippi, 297 U.S. 278, 287 (1936) (holding a confession in state court inadmissible under the due process clause).

[113] An enormous array of articles discuss personal jurisdiction in connection with Internet transmissions. *See*, *e.g.*, Yvonne A. Tamayo, *Who? What? When? Where?: Personal Jurisdiction and the World Wide Web*, 4 RICH. J.L. & TECH. 7 (Spring 1998), *at* http://www.richmond.edu/jolt/v4i3/tamayo.html; Brian E. Daughdrill, *Personal Jurisdiction And The Internet: Waiting For The Other Shoe To Drop On First Amendment Concerns*, 51 MERCER L. REV. 919 (2000); Katherine Neikirk, *Note, Squeezing Cyberspace Into International Shoe: When Should Courts Exercise Personal Jurisdiction Over Noncommercial Online Speech?*, 45 VILL. L. REV. 353 (2000); Kevin R. Lyn, *Personal Jurisdiction And The Internet: Is A Home Page Enough To Satisfy Minimum Contacts?*, 22 CAMPBELL L. REV. 341 (2000); Sean M. Flower, Note, *When Does Internet Activity Establish The Minimum Contact Necessary To Confer Personal Jurisdiction?*, 62 MO. L. REV. 845 (1997); David L. Stott, Comment, *Personal Jurisdiction In Cyberspace: The Constitutional Boundary Of Minimum Contacts Limited To A Web Site*, 15 J. MARSHALL J. COMPUTER &

INFO. L. 819 (1997).

[114] *Cf*. Burnham v. Superior Court, 495 U.S. 604 (1990) (presenting a situation arguably involving jurisdiction based on transitory presence, but not resulting in an opinion for the Court on this point).

[115] 339 U.S. 763 (1950).

[116] *Id*. at 784.

[117] United States v. Doe, 465 U.S. 605, 616 (1984).

[118] United States v. Verdugo-Urquidez, 494 U.S. 259, 261 (1990).

[119] *Id*. at 264.

[120] *Id*. at 264-65.

[121] 367 U.S. 643 (1961).

[122] Lustig v. United States, 338 U.S. 74, 78-79 (1949) (plurality opinion) (Frankfurter, J.). Frankfurter provides the origin of this phrase in his statement that "the crux of that doctrine is that a search is a search by a federal official if he had a hand in it; it is not a search by a federal official if evidence secured by state authorities is turned over to the federal authorities on a silver platter." *Id*. *See* Elkins v. United States, 364 U.S. 206, 207 n.1 (1960).

[123] *Elkins*, 364 U.S. at 223.

[124] Rea v. United States, 350 U.S. 214 (1956).

[125] *See* United States v. Balsys, 524 U.S. 666, 698 (1998).

[126] United States v. Hubbell, 167 F.3d 552, 581 (D.C. Cir. 1999).

[127] *See* United States v. Hubbell, 530 U.S. 27, 33-34 (2000).

[128] *E.g*., Berger v. New York, 388 U.S. 41, 98 (1967); Weeks v. United States, 232 U.S. 383, 393-94 (1914).

[129] 920 F. 2d 940 (D.C. Cir. 1990).

[130] *Id*. at 942.

[131] *See* 167 F.3d at 580 n.34 (citing Terry v. Ohio, 392 U.S. 1, 21-24 (1968); Alabama v. White, 496 U.S. 325, 330 (1990)).

[132] Verdugo-Urquidez, 494 U.S. at 264 (quoting United States v. Calandra, 414 U.S. 338, 354 (1974); United States v. Leon, 468 U.S. 897, 906 (1984)).

[133] *Id*. (citing Malloy v. Hogan, 378 U.S. 1 (1964); Kastigar v. United States, 406 U.S. 441, 453 (1972)) (emphasis added).

[134] *E.g*., Nix v. Williams, 467 U.S. 431, 442-43 (1984).

[135] *Id*. *See also* Murray v. United States, 487 U.S. 533, 537 (1988) (distinguishing the attenuation exception to the Fourth Amendment's exclusionary rule from the independent source exception, which applies to evidence acquired not only through Fourth Amendment violations but also through Fifth and Sixth Amendment violations).

[136] *Kastigar*, 406 U.S. at 461.

[137] United States v. Hubbell, 167 F.3d 552, 602 (D.C. Cir. 1999) (citing *Kastigar*, 406 U.S. at 461).

[138] *Kastigar*, 406 U.S. at 461-62.

[139] United States v. Hubbell, 530 U.S. 27, 42-46 (2000) (citing *Fisher*, 425 U.S. at 394).

[140] *Id*. at 2050 (Thomas, J., concurring).

[141] *Id*.

[142] *Id*. at n.1.

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

[144] *Hubbell,* 530 U.S. at 56 (Thomas, J., concurring). *See also* Sergienko, *supra* note 1, at ¶ 24.

[145] Sergienko, *supra* note 1, at ¶ 19-21.

[146] *See* Schmerber v. California, 384 U.S. 757 (1966).

[147] *Id*. at 761.

[148] *See id*. at 774 (Black, J., dissenting). The analysis of testimoniality in Justice Brennan's opinion for the *Schmerber* majority may be considered an alternative holding, because Justices Harlan and Stewart, who constituted two of the majority's five votes, thought that there was no Fifth Amendment issue at all, apparently because they believed the amendment applied only to compelled, in-court testimony. *See id*. at 772 (Harlan, J., concurring) (citing Miranda v. Arizona, 484 U.S. 436, 526 (1966) (White, J., joined by Harlan, J., dissenting)).

[149] *Hubbell*, 530 U.S. at 50 (Thomas, J., concurring).

[150] *Id*. at 50-51.

[151] *See id*. & n.2.

[152] *Id*. at 51.

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

[154] *See* Schmerber v. United States, 384 U.S. 757 (1966).

[155] *See* Boyd v. United States, 116 U.S. 616, 634-35 (1886). 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).

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

[157] *Id*.

[158] United States v. Hubbell, 530 U.S. 27, 49 (2000) (Thomas, J., concurring).

[159] United States v. Hubbell, 167 F.3d 552, 581 (U.S. App. D.C. 1999), *aff'd* 530 U.S. 27 (2000).

[160] U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and *particularly describing the place to be searched, and the persons or things to be seized*.") (emphasis added).

[161] "Where possession cannot be independently shown, common sense and experience suggest that incriminating evidence frequently will not be produced." Alito, *supra* note 27, at 47.

[162] Froomkin, *supra* note 14, at 887-89. As Froomkin observes, brute-force decryption requires identifying the method of encryption. *Id*. Where someone has seized the computer encrypting the ciphertext, identifying the method of encryption will be relatively easy, because the computer program that encrypts must be decrypted itself in order to work. Where the message has been intercepted, the need to try a variety of methods of encryption will greatly complicate the task of decrypting the document.

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

[164] 116 U.S. 616 (1886).

[165] *Id*. at 634-35.

[166] 387 U.S. 294, 301-02 (1967).

[167] *See* Boyd, 116 U.S. at 622-33. *See generally* Sergienko, *supra* note 1, at ¶¶ 44-45.

[168] *E.g*., United States v. R. Enterprises, Inc., 498 U.S. 292, 301 (1991) (holding that a grand jury's subpoena is presumed relevant and will be upheld unless "there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation"). Grand juries are free to "act on tips, rumors, evidence offered by the prosecutor, or their own personal knowledge," United States v. Dionisio, 410 U.S. 1, 15 (1973). *Dionisio* also affirmed the rule that a grand jury witness "is not entitled to set limits to the investigation that the jury may conduct." *Id*. (quoting Blair v. United States, 250 U.S. 273, 282 (1919)).

[169] *E.g*., Dawn Piimanu, *Prying Eyes*, CYBER ESQ., Winter 2000, at 26.

[170] *Id*. at 28 (statement of Donald Kerr, assistant director of the FBI's Laboratory Division).

[171] *Id*. at 26 (statement of David Sobel, general counsel of the Economic Privacy Information Center).

[172] *See* Fisher v. United States, 425 U.S. 391, 407 (1976).

[173] *See* Reitinger, *supra* note 4.

Related Browsing

1. http://www.abanet.org/lpm/newsarticle11130_front.shtml. "Confidentiality in an Electronic World Using Encryption in Everyday Law Practice." This site contains information about how encryption works and about the malpractice and ethical issues that may arise in the context of encryption.

2. http://www.epic.org/crypto/. "Electronic Privacy Information Center." This site contains updates about recent cases dealing with Internet privacy, administrative agency decisions and policies regarding Internet privacy, and links to the full text of relevant documents and court decisions.

3. http://www.aclu.org/issues/cyber/priv/priv.html. "Cyber-liberties." This site contains information about encryption and links to relevant briefs, articles, and ACLU comments.

4. http://www.privacyresources.com/. "Internet Privacy and E-mail Security." This site contains background information about encryption, how it works, why it is important, and the risks involved if encryption is not used.

5. http://www.stardot.com/~lukeseem/j202/. "Keys to Secret Drawers: The Clipper Chip and Key Escrow Encryption." This site contains an essay about the government's problem of promoting encryption and gathering criminal information.

6. http://www.findarticles.com/m0MCW/7_17/64339850/p1/article.jhtml. "Protect Your E-mail." This article discusses the privacy risks involved with using e-mail and what users can do to decrease that risk.

7. http://www.arawak.net/pages/privacy.index.html. "Arawak Net's Internet Privacy Watch." This site contains links to articles dealing with many different aspects of Internet privacy, including private and public key encryption, digital signatures, and how "cookies" affect privacy.

8. http://www.cs.auckland.ac.nz/~pgut001/tutorial/index.html. "Godzilla Crypto Tutorial" by Peter Gutmann, Department of Computer Science, University of Auckland, Private Bag 92019, Auckland, New Zealand. Gives an excellent description of cover security threats and requirements, services and mechanisms, historical ciphers, assorted block, stream, and public-key ciphers, hash functions, and signature algorithms.

9. http://businessweek.lycos.com/smallbiz/content/apr2000/gg000419.htm. "A Chinese Puzzle: What Do Beijing's Net Policies Mean?" An article that discusses encryption issues and the Chinese government's declaration that commercial encryption codes "part of national classified information."

10. http://news6.thdo.bbc.co.uk/hi/english/special_report/1998/encryption/newsid_57000/57910.stm. "The great encryption debate." The government and the technology community are butting heads over encryption. National security or the empowerment of Big Brother? Opposing forces in the great encryption battle say that it is going to be one or the other.

11. http://world.std.com/~franl/crypto/. Cryptography: The Study of Encryption.
