Vanderbilt Journal of Entertainment & Technology Law

Volume 12
Issue 3 *Issue 3 - Spring 2010*

Article 4

2010

# The Weak Protection of Strong Encryption: Passwords, Privacy, and Fifth Amendment Privilege

Nathan K. McGregor

Recommended Citation

Nathan K. McGregor, The Weak Protection of Strong Encryption: Passwords, Privacy, and Fifth Amendment Privilege, 12 *Vanderbilt Journal of Entertainment and Technology Law* 581 (2020)
Available at: https://scholarship.law.vanderbilt.edu/jetlaw/vol12/iss3/4

# The Weak Protection of Strong Encryption: Passwords, Privacy, and Fifth Amendment Privilege

## ABSTRACT

*While the constitutional protection afforded private papers has waxed and waned for more than a century, the Supreme Court has greatly restricted the Fifth Amendment privilege against self-incrimination—at least as applied to voluntarily prepared documents. Specifically, where the government knows of the existence and location of subpoenaed documents, the Fifth Amendment guarantee will not justify a failure to produce them, unless the act of production would itself incriminate the defendant. However, the Self-Incrimination Clause still precludes the compelled creation of documents that are both incriminating and testimonial.*

*The "private papers" doctrine has remained relatively stable for approximately thirty years now, even though most documents—including private "papers"—presumably exist on various digital media, the retrieval of which require sophisticated, if ubiquitous, technology. Arguably, encrypted documents do not comport well with the general rule that discoverable materials must be produced in a readable format. Few courts have ruled on motions to quash subpoenas for encrypted files, and each has simply applied the private papers doctrine with no discussion of whether encrypted documents warrant special protection. While the decisions in these cases are reasonable enough, decryption by court order would at least appear to compel incriminating testimony—contrary to the Fifth Amendment.*

*Though unstated in the opinions, these courts may have agreed with the many companies and commentators who compare the encryption of documents to their placement in a locked safe. While merely sequestering documents clearly does not protect them from a valid subpoena, this simple analogy fails to capture several important features of encryption. This Note considers an alternative conceptualization that, while less intuitive, more accurately reflects these important features. Under this paradigm, the private papers doctrine probably still applies to encrypted contraband, but courts should not adhere to an inappropriate analogy in any event. Ideally,*

*the Supreme Court would expressly grant encrypted documents no greater protection under the Fifth Amendment than that currently afforded traditional private papers.*

## TABLE OF CONTENTS

The following situation frequently confronts law enforcement officers from any number of government agencies.[1] As part of a raid or routine inspection, an officer discovers images of child pornography or other contraband on a computer. Sometimes the officer expects to find the contraband—sometimes not. The person in possession of the computer often cooperates, at least initially, freely revealing the illicit files to the agent. With or without a warrant, the officer seizes the computer, but inadvertently or improperly closes the files or shuts down the computer. When the investigator or prosecutor attempts to view the illegal material, either the file cannot be found at all, or it cannot be opened because the file or the hard drive has automatically

[1] See, for example, the facts of the *Boucher* case discussed *infra* Part I.C.2. At least in Nashville, a diverse panoply of law enforcement agencies have joined the fight against child pornography. They include: Federal Bureau of Investigation, Franklin Police Department Internet Crimes Against Children Unit, Tennessee Association of Chiefs of Police, Tennessee Bureau of Investigation, United States Secret Service, and United States Attorney's Office—all of which sponsored a recent conference attended by the author: Identifying Online Child Exploitation Crimes, held at the Nashville State Community College (Cookeville Campus) on July 23, 2009.

encrypted. With time to grasp the gravity of his situation, and perhaps on the advice of a lawyer, the owner of the computer declines further cooperation. Now the law enforcement agency faces a dilemma, as its case against the suspect requires either a decrypted version of the now encrypted file or the key to effect that decryption.[2] Without the key, cracking the code could easily require many years of computer time.[3] If the suspect refuses to provide an unencrypted version of the document (or the key) voluntarily, then the prosecutor may resort to the subpoena power of a grand jury.[4]

Whether such subpoenas are valid remains somewhat unclear because no appellate court has yet ruled on the discoverability of encrypted documents via grand jury subpoenas. The only trial courts to rule on the issue, both within the Court of Appeals for the Second Circuit, have simply applied precedent for (unencrypted) "private papers" to the situation at hand.[5] In both cases, the courts found the contested subpoena was (or would be) valid, if (and only if) the government could independently authenticate the files,[6] the existence and location of which were already known to the government.[7] Each court found that the files had been voluntarily created, which rendered their *content* exempt from Fifth Amendment protection;[8]

[2] See *infra* Part II.A for an overview of encryption.

[3] As discussed in Part II.A, *infra*, decryption generally requires the "factoring" of enormous numbers. Even the most powerful of computers require years to solve such mathematical problems. For example, factoring a 664-bit number by networking one million computers—each performing one million operations per second—would require some four thousand years. *See* Phillip R. Reitinger, *Compelled Production of Plaintext and Keys*, 1996 U. CHI. LEGAL F. 171, 175 n.19 (1996) (citing BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C, 284 n.11 (2d. ed. 1996)). However, such tasks are hardly impossible; indeed, an even larger number has recently been factored with "many hundreds" of computers working in tandem for nearly two years. *See* Thonsten Kleinjung et al., *Factorization of a 768-bit RSA modulus* (January 13, 2010), *available at* http://eprint.iacr.org/2010/006.pdf.

[4] *See generally* WAYNE R. LAFAVE ET AL., 3 CRIM. PROC. § 8.4(b) (3d ed. 2007).

[5] *In re* Grand Jury Subpoena to Sebastian Boucher, No. 2:06-mj-91, 2009 U.S. Dist. LEXIS 13006 (D. Vt. Feb. 19, 2009); United States v. Pearson, No. 1:04-CR-340, 2006 U.S. Dist. LEXIS 32982 (N.D.N.Y. May 24, 2006), *aff'd*, 570 F.3d 480 (2d Cir. 2009); *see infra* Part I.C.

[6] *See* FED. R. EVID. 901(a) ("The requirement of authentication . . . is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."); *See generally*, CHRISTOPHER B. MUELLER & LAIRD KIRKPATRICK, EVIDENCE UNDER THE RULES (6th ed. 2008).

[7] *See Boucher*, 2009 U.S. Dist. LEXIS 13006, at *9-*10; *Pearson*, 2006 U.S. Dist. LEXIS 32982, at *58-*59, *62.

[8] *See Boucher*, 2009 U.S. Dist. LEXIS 13006, at *6; *Pearson*, 2006 U.S. Dist. LEXIS 32982, at *62.

thus, the entire analysis in each opinion considered whether the *act* of production would invoke the privilege.[9]

Unquestionably, the documents (believed to be images of child pornography) were created voluntarily in these cases,[10] so that—had the files remained unencrypted—this analysis would be squarely on point. Both courts apparently ignored a disquieting detail though, which arguably renders this analysis irrelevant: if, upon encryption, the original document ceases to exist, then forcing the target of a subpoena to provide an unencrypted version would appear to compel the creation of a new and incriminating document, which contravenes Supreme Court jurisprudence on the Self-Incrimination Clause.[11]

While this argument probably fails in the end, it at least warrants an analysis.[12] Though not explicit in the opinions, the district courts may have conceptualized encryption in the same way that many security companies, legal commentators, and even the targets of subpoenas apparently have—as the placement of documents in a locked safe.[13] This analogy does capture a few characteristics of encryption, but it fails to account for several others. In particular, placing documents in a safe obviously leaves their content intact, while encryption alters the content of the original text in a meaningful sense.[14] The former system protects information by physically sequestering it—and nothing more—while encryption scrambles the message itself. This distinction renders comparisons with safes inappropriate.[15]

This Note proposes an alternative analogy that more accurately embodies the important features of encryption.[16] The proposed paradigm casts at least some doubt on the propriety of deeming "voluntary" the compelled decryption of previously voluntarily created but encrypted documents, at least when the encrypted "document" consists of pure contraband.[17] While this

[9] *See Boucher*, 2009 U.S. Dist. LEXIS 13006, at *6-*10; *Pearson*, 2006 U.S. Dist. LEXIS 32982, at *53-*63.

[10] *See Boucher*, 2009 U.S. Dist. LEXIS 13006, at *6 ("There is no question that the contents of the laptop were voluntarily prepared or compiled [by the defendant] and are not testimonial, and therefore do not enjoy Fifth Amendment protection."); *Pearson*, 2006 U.S. Dist. LEXIS 32982, at *60 ("Defendant has already voluntarily asserted under oath that the seized files contain *his* material.").

[11] *See infra* Part I.A.

[12] *See infra* Parts II and III.

[13] *See infra* note 66 and accompanying text.

[14] *See infra* Part II.A.

[15] *See infra* Part II.B.2.

[16] *See infra* Part II.B.3.

[17] *See infra* Part III.

argument may ultimately prove unpersuasive, it suggests that courts' extension of the "private papers" jurisprudence to encrypted documents has stretched that common law doctrine a little too thin.[18] The Supreme Court should address this issue directly and, in the interest of public policy, clarify that encrypted documents warrant no more (and contraband perhaps even less) protection under the Fifth Amendment than other private papers.

Part I of this Note traces the development of the private papers doctrine, as articulated by the Supreme Court, interpreted by the Court of Appeals for the Second Circuit, and applied to encrypted documents by two district courts within the Second Circuit. Part II includes a brief, non-technical overview of encryption, examines two common analogies with which it is often described, and suggests an alternative comparison that better captures its unique features. Part III considers whether the private papers doctrine should cover encrypted documents, particularly contraband, under the rubric of the proffered analogy. Part IV concludes that current doctrine probably survives under the new paradigm, but in no event should additional Fifth Amendment protection attach to encrypted documents.

## I. "PRIVATE PAPERS" AND THE SELF-INCRIMINATION CLAUSE

### *A. The Supreme Court's Framework*

The Fifth Amendment provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself."[19] The populist belief that liberty should preclude private papers from government seizure found judicial sanction in *Entick v. Carrington.*[20] This English case, which predated the American Revolution, laid the conceptual foundation for generous Fifth Amendment protection, as first articulated by the U.S. Supreme Court in *Boyd v. United States.*[21] The Court in *Boyd* reversed a civil forfeiture where the defendants, charged with avoiding the prescribed duty on imported glass, had

[18] Part I.A, *infra*, outlines the "private papers" doctrine; Part III, *infra*, discusses the extension of this doctrine to encryption.

[19] U.S. CONST. amend. V.

[20] Entick v. Carrington, [1765] 95 Eng. Rep. 807 (K.B.) (holding that the seizure of private papers by government officials—absent statutory or common law authority—constitutes an illegal trespass, lest "the secret cabinets and bureaus of every subject in this kingdom . . . be thrown open to the search and inspection of a messenger, whenever the secretary of state shall think fit to charge, or even to suspect, a person to be the author, printer, or publisher of a seditious libel."), *available at* http://www.constitution.org/trials/entick/entick_v_carrington.htm.

[21] Boyd v. United States, 116 U.S. 616 (1886) (quoting extensively from, and relying on, Lord Camden's opinion for the High Court in *Entick*).

produced incriminating invoices under the compulsion of a court order.[22]

In so ruling, the Court apparently conflated the Fifth Amendment privilege against self-incrimination with protections found only in the Fourth[23]: "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."[24] For decades, the Court equivocated on whether analysis under the Fourth Amendment necessarily implicated the Fifth.[25] Although subsequent decisions significantly curtailed the broad scope of *Boyd*,[26] its central holding that Fifth Amendment principles protect private papers from government compulsion regularly appeared as dictum in Court opinions for more than eighty years.[27] Indeed, uncertainty as to the continued validity of *Boyd* lingered for at least a century.[28]

In *Fisher v. United States*, the Supreme Court markedly narrowed its Fifth Amendment jurisprudence.[29] In a landmark decision,[30] the majority found no Self-Incrimination Clause protection for taxpayers who defied summonses from the Internal Revenue Service directing them to produce tax returns prepared by their accountants.[31] Characterizing the preparation of these documents as

[22] *Id.* at 537.

[23] 1 MCCORMICK ON EVIDENCE § 127, at 183 (John W. Strong et al. eds., 4th ed. 1992); CHRISTOPHER SLOBOGIN, CRIMINAL PROCEDURE: REGULATION OF POLICE INVESTIGATION 180 (4th ed. 2007) (noting that subsequent decisions "returned to *Boyd*'s mix of the fourth and fifth amendment rationales.").

[24] U.S. CONST. amend. IV.

[25] *Compare* Weeks v. United States, 232 U.S. 383 (1914) (rejecting immunity under all circumstances for private papers without relying on the Fifth Amendment), *with* Gouled v. United States, 255 U.S. 309 (1921) (holding that search warrants "may not be used as a means of gaining access to a man's house or office and papers solely for the purpose of making search to secure evidence to be used against him in a criminal or penal proceeding.").

[26] *E.g.*, Shapiro v. United States, 335 U.S. 1, 7 (1948) (government may subpoena legislatively mandated business records).

[27] *In re* Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992, 1 F.3d 87, 91 (2d Cir. 1993) (citing Bellis v. United States, 417 U.S. 85 (1974), Schmerber v. California, 384 U.S. 757 (1966), United States v. White, 322 U.S. 694 (1944), and Wilson v. United States, 221 U.S. 361 (1911)); *see also id.* at 95 (Altimari, J., dissenting) (citing Couch v. United States, 409 U.S. 322 (1973)).

[28] *Id.* at 95 (Altimari, J., dissenting) ("In sum, although *Boyd*'s continued vitality has been questioned, its pronouncement that personal papers are protected by the Fifth Amendment has never been expressly overruled.").

[29] Fisher v. United States, 425 U.S. 391, 409 (1976) (without dissent).

[30] Robert P. Mostellar, *Simplifying Subpoena Law: Taking the Fifth Amendment Seriously*, 73 VA. L. REV. 1, 3 (1987) (calling *Fisher* a "major watershed, signaling a fundamental departure from earlier Fifth Amendment doctrines.").

[31] *Fisher*, 425 U.S. at 409.

"wholly voluntary," the Court found antithetical the petitioners' claim of compulsion.[32] Subsequent decisions reiterated this limitation on Fifth Amendment protection that only the compelled creation of documents would render their content inadmissible.[33] *Fisher* preserved Fifth Amendment protection only against the production—not the substance—of compelled, incriminating testimony.[34]

In reaffirming *Fisher*, later Courts emphasized that private papers do not invoke the privilege merely because their content would tend to incriminate the defendant.[35] In *United States v. Doe*, Justice O'Connor wrote separately to stress that "the Fifth Amendment provides absolutely no protection for the contents of private papers of any kind."[36] The Supreme Court next considered the issue in *Baltimore Department of Social Services v. Bouknight*.[37] While *Bouknight* involved the production of a child, rather than private papers, the Court cited with approval Justice O'Connor's concurrence in *Doe*.[38] Whether her stringent position has attained the status of binding precedent remains unclear,[39] and lower courts have been left to extrapolate the precise contours of the Supreme Court's jurisprudence on this issue.[40]

In rejecting the last vestiges of *Boyd*, the U.S. Court of Appeals for the Second Circuit reasoned that, while no other member of the

[32] *Id.*

[33] United States v. Doe, 465 U.S. 605, 612 n.10 (1984) ("If the party asserting the Fifth Amendment privilege has voluntarily compiled the document, no compulsion is present and the contents of the document are not privileged.").

[34] *Fisher*, 425 U.S. at 410 n.11 ("In the case of a documentary subpoena, the only thing compelled is the act of producing the document and the compelled act is the same as the one performed when a . . . document not authored by the producer is demanded.") (citing 1 MCCORMICK ON EVIDENCE § 128, at 269 (4th ed. 1992)).

[35] Baltimore Dep't of Social Servs. v. Bouknight, 493 U.S. 549, 555 (1990) ("[A] person may not claim the [Fifth] Amendment's protections based upon the incrimination that may result from the contents or nature of the thing demanded.").

[36] United States v. Doe, 465 U.S. at 618 (O'Conner, J., concurring).

[37] *Bouknight*, 493 U.S. 549 (1990).

[38] *Id.* at 555.

[39] *Doe*, 465 U.S. at 619.

> Contrary to what Justice O'Connor contends . . . I do not view the Court's opinion in this case as having reconsidered whether the Fifth Amendment provides protection for the contents of "private papers of any kind." This case presented nothing remotely close to the question that Justice O'Connor eagerly poses and answers. First, . . . the issue whether the Fifth Amendment protects the contents of the documents was obviated by the Court of Appeals' ruling relating to the act of production and statutory use immunity. Second, the documents at stake here are business records which implicate a lesser degree of concern for privacy interests than, for example, personal diaries.

*Id.* (Marshall, J., concurring in part and dissenting in part) (footnotes omitted).

[40] See *infra* Part I.C for cases applying this doctrine to encrypted documents.

Court joined in Justice O'Connor's opinion, "the decision in *Bouknight* suggests that a majority of the Court now agrees with her position."[41] In the same opinion, the Second Circuit neatly summarized the paradigm shift from the relics of *Boyd* to *Fisher* and its progeny:

> The Court no longer views the Fifth Amendment as a general protector of privacy or private information, but leaves that role to the Fourth Amendment. Self-incrimination analysis now focuses on whether the creation of the thing demanded was compelled, and, if not, whether the act of producing it would constitute compelled testimonial communication.[42]

In its most recent decision directly on point, the Supreme Court appears to have followed this Second Circuit opinion—though without explicitly citing it.[43] With no negative history at all, and a substantial following of district court decisions in its wake, this Second Circuit case remains good law and warrants close inspection.

### *B. The Second Circuit's Interpretation*

The Second Circuit implemented the *Fisher* framework with a two-prong test.[44] In *In re Grand Jury Subpoena*, the defendant (known only as John Doe), responded to an investigation by the Securities and Exchange Commission (SEC) by providing the government with a copy of his personal datebook.[45] Federal prosecutors, having obtained this reproduction from the SEC, became suspicious that Doe had blotted out certain entries before photocopying the pages.[46] A grand jury, which had convened to consider charges of perjury and obstruction of justice, issued a subpoena directing the defendant to produce the original version of

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

[42] *Id.* at 93 (citations omitted).

[43] *Compare* United States v. Hubbell, 530 U.S. 27, 45 (2000) ("[T]he act of producing documents in response to a subpoena may have a compelled testimonial aspect. . . . By 'producing documents in compliance with a subpoena, the witness would admit that the papers existed, were in his possession or control, and were authentic.'") (quoting *Doe*, 465 U.S. at 613), *with In re* Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992, 1 F.3d at 93 ("While the contents of voluntarily prepared documents are not privileged, the act of producing them in response to a subpoena may require incriminating testimony in two situations: (1) 'if the existence and location of the subpoenaed papers are unknown to the government'; or (2) where production would 'implicitly authenticate' the documents.") (quoting United States v. Fox, 721 F.2d 32, 36 (2d Cir. 1983)).

[44] *In re* Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992, 1 F.3d at 93.

[45] *Id.* at 89.

[46] *Id.*

the datebook.[47] While objecting to the subpoena, the defendant nevertheless allowed the government to examine the calendar.[48]

Despite the apparent doctoring of key entries, the district judge denied the government's motion to compel production of the datebook, apparently finding its substance protected by the Self-Incrimination Clause:

> [T]he content of the original document as originally written or revised was not published to anyone; the disclosure of a purported copy to the SEC was not a publication of the original; the original document was not voluntarily disclosed to the SEC or to the Assistant United States Attorney. The original document is subject to the privilege of the Fifth Amendment in its original and its present altered (if it was) form.[49]

On appeal, though, a panel of Second Circuit judges carefully traced the line of Supreme Court cases from *Boyd* to *Bouknight* and concluded that "because Doe voluntarily prepared the calendar, its contents are not protected by the Fifth Amendment."[50]

Citing its own precedent, the appeals court acknowledged that a subpoena may compel incriminating testimony—in violation of the Fifth Amendment—in two situations: "(1) 'if the existence and location of the subpoenaed papers are unknown to the government';[51] or (2) where production would 'implicitly authenticate' the documents."[52] Hence, where the government can independently authenticate documents, including private papers, known to exist in a particular place, the Fifth Amendment privilege affords absolutely no protection from an otherwise valid subpoena.[53]

[47] *Id.*

[48] *Id.*

[49] *Id.* at 90.

[50] *Id.* at 93 (emphasis added).

[51] *Id.* (quoting United States v. Fox, 721 F.2d 32, 36 (2d Cir. 1983)). Conversely, "[p]roduction may not be refused 'if the government can demonstrate with reasonable particularity that it knows of the existence and location of subpoenaed documents.'" *Id.* (quoting *In re* Grand Jury Subpoena Duces Tecum Dated Nov. 13, 1984, 616 F. Supp. 1159, 1161 (E.D.N.Y. 1985)).

[52] *Id.* (quoting *In re* Grand Jury Subpoena Duces Tecum Dated Nov. 13, 1984, 616 F. Supp. 1159, 1161 (E.D.N.Y. 1985)).

[53] However, Justice Thomas (joined by Justice Scalia) has signaled his willingness to reconsider Fifth Amendment protection, the current (narrow) interpretation of which he views as inconsistent with the Founders' intent. *See* United States v. Hubbell, 530 U.S. 27, 49 (2000) (Thomas, J., concurring) ("A substantial body of evidence suggests that the Fifth Amendment privilege protects against the compelled production not just of incriminating testimony, but of any incriminating evidence. In a future case, I would be willing to reconsider the scope and meaning of the Self-Incrimination Clause."). *But see* Donald Dripps, *Self-Incrimination, in* THE HERITAGE GUIDE TO THE CONSTITUTION 335, 335-36 (David Forte et al. eds., 2005) ("The Founders . . . regarded the privilege as valuable enough to include in the Constitution, but their own practice [of pretrial questioning by a magistrate] put considerable pressure on defendants to surrender incriminating information before trial."). Over the last half-century, conservative justices have generally sought to circumscribe—if not actually reverse—the robust rights,

In considering the facts before it, the appellate court found neither the particularity nor the authentication prong of its test satisfied.[54] The defendant had undeniably possessed and controlled the calendar; indeed, he had previously testified to that effect and produced a copy of the original.[55] Thus, having openly owned the datebook, "its existence and location are 'foregone conclusions,' and his production of the original 'adds little or nothing to the sum total of the Government's information.'"[56] As for authentication, the government could establish that Doe had already submitted a photocopy, and it could then allow jurors to compare that reproduction with the original document. "Accordingly, because Doe's compliance with the subpoena would require mere 'surrender' of the calendar, and not 'testimony,' Doe has no act of production privilege."[57] Finding neither prong applicable, the Second Circuit reversed the district court's denial of the government's motion to compel production of the calendar.[58]

### *C. District Courts Apply "Private Papers" to Encrypted Files*

Recent cases, while extremely sparse, provide important insight as to how trial courts have applied the Supreme Court's Self-Incrimination Clause jurisprudence—with its emphasis on private papers—to encrypted computer files, at least through the filter of Second Circuit precedent. [59]

#### 1. Authentication

In *United States v. Pearson*, the defendant faced multiple charges, such as producing, distributing, receiving, and possessing

particularly Fifth Amendment protections, gradually afforded criminal defendants during this period. *See* LAWRENCE M. FRIEDMAN, A HISTORY OF AMERICAN LAW 572 (3d. ed., 2007).

[54] *In re* Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992, 1 F.3d at 90 ("Because neither of these situations exist here, Doe has no act of production privilege.").

[55] *Id.* at 89.

[56] *Id.* at 93 (2d Cir. 1993) (quoting Fisher v. United States, 425 U.S. 391, 411 (1976)).

[57] *Id.* at 93-94.

[58] *Id.* at 88.

[59] *In re* Grand Jury Subpoena to Sebastian Boucher, No. 2:06-mj-91, 2009 U.S. Dist. LEXIS 13006 (D. Vt. Feb. 19, 2009); United States v. Pearson, No. 1:04-CR-340, 2006 U.S. Dist. LEXIS 32982 (N.D.N.Y. May 24, 2006), *aff'd*, 570 F.3d 480 (2d Cir. 2009). Outside of the Second Circuit, no other court has directly addressed the issue of when the government may compel passwords to access encrypted files. Such a scarcity of case law seems unlikely to persist, however, as encryption software becomes cheaper, stronger, and easier to implement. In particular, those who trade in child pornography, often adept users of computer technology, will inevitably exploit encryption with ever increasing frequency. As the issue confronts more courts, judges will presumably consider the limited case law from the Second Circuit. Whether that precedent will prove persuasive in other jurisdictions, however, remains to be seen.

child pornography.[60] While still preparing for trial, the government learned that Pearson, having made bail, had reacquired the very images originally confiscated.[61] Obtaining a search warrant, the government seized computer equipment belonging to Pearson's father, an attorney with whom the defendant now lived.[62]

During a forensic examination of these materials, the Federal Bureau of Investigation (FBI) found encrypted files in a folder labeled "steganosencryptionsafes."[63] The investigation also uncovered an email from "staganos.asknet.de" to an America Online alias registered to the defendant ("Peall2065").[64] The message included a password and serial number enabling him to download encryption software.[65] One week later, "Peall2065" (also known as "Ov") emailed a confidant: "Ov has a "safe" for securing data & will change his password then so that no computer or human can retrieve saved data. The thing encrypts immediately (live/realtime) and will have a password like: eolKleGH93*vfO&3Gw4kn&jd."[66]

[60] *Pearson*, 2006 U.S. Dist. LEXIS 32982, at *1; *See* United States Criminal Code, Sexual Exploitation and Other Abuse of Children, Sexual Exploitation of Children, 18 U.S.C. § 2251(a) (2009) (production); United States Criminal Code, Sexual Exploitation and Other Abuse of Children, Certain Activities Relating to Material Involving the Sexual Exploitation of Minors, 18 U.S.C. § 2252A(a)(1) (2009) (distribution); United States Criminal Code, Sexual Exploitation and Other Abuse of Children, Certain Activities Relating to Material Involving the Sexual Exploitation of Minors, 18 U.S.C. § 2252A(a)(2) (2009) (receipt); United States Criminal Code, Sexual Exploitation and Other Abuse of Children, Certain Activities Relating to Material Involving the Sexual Exploitation of Minors, 18 U.S.C. § 2252A(a)(5)(b) (2009) (possession). The stakes are extremely high in these cases: even a first time offender faces a *mandatory* minimum sentence of five years imprisonment for receipt or distribution of child pornography; production of the same carries a fifteen-year minimum. *See id.* Recently, a small but significant minority of federal judges have openly resisted the imposition of such penalties, deeming them unnecessary and unjust. *Compare* Mark Hansen, *A Reluctant Rebellion*, ABA JOURNAL, June 2009, at 54-59, *available at* http://www.abajournal.com/magazine/article/a_reluctant_rebellion, *with* Alexandra Gelber, *A Response to* A Reluctant Rebellion, U.S. Department of Justice (July 1, 2009), *available at* http://www.justice.gov/criminal/ceos/ReluctantRebellionResponse.pdf.

[61] *Id.* at *6-*8.

[62] *Id.*

[63] For the latest "Safe" offered by Steganos, see *infra* note 66.

[64] *Pearson*, 2006 U.S. Dist. LEXIS 32982, at *13.

[65] PGP software is widely available. *See, e.g.*, International PGP Homepage, Freeware, http://www.pgpi.org/products/pgp/versions/freeware (last visited Feb. 15, 2009) (listing more than 100 freeware versions of PGP available for download). Phil Zimmermann created the encryption system "Pretty Good Privacy" (or PGP) in 1991. International PGP Homepage, History, http://www.pgp.com/about_pgp_corporation/history.html (last visited Feb. 15, 2009). For background information on another "public key" encryption system—RSA (named for Rivest, Shamir, and Adleman, the mathematicians who invented it)—see *infra* note 110 and accompanying text.

[66] *Pearson*, 2006 U.S. Dist. LEXIS 32982, at *7. Many commentators have analogized encryption to a safe. *See, e.g.*, Reitinger, *supra* note 3, at 173-78. Commercial providers of encryption software also embrace this analogy. Steganos advertises the latest version of its product—literally called "Safe"—with an explicit comparison: "Works like a real safe to protect

On one of the seized hard drives, the forensic examination uncovered an encrypted 2.3 gigabyte folder—large enough to contain many image files.[67] While the FBI suspected that these files depicted sexually explicit images of minors, encryption thwarted the investigation.[68] For this reason, the government obtained a subpoena demanding the production of all relevant passwords at trial.[69] The defendant moved to quash on grounds that his Fifth Amendment privilege extended to producing passwords.[70]

The government argued that the arbitrary nature of such a password precludes Fifth Amendment protection of its content for two reasons.[71] First, an inherently meaningless string of characters cannot itself convey incriminating information.[72] Second, such a long sequence of random symbols would prove difficult to memorize, suggesting the defendant likely wrote it down—and Fifth Amendment protection excludes voluntarily produced writings.[73] Pearson apparently failed to rebut either of these arguments, thus conceding this important point.[74]

Even assuming that the Self-Incrimination Clause exempts from its protection any content a password may embody, the defendant nevertheless claimed his act of production would still lie within its scope.[75] After summarizing the Supreme Court and Second Circuit precedent, the district judge applied law to facts:

> [C]ompliance with the subpoena does not tacitly concede the existence or location of the computer files because the files are already in the Government's possession. Their existence is a foregone conclusion. Further, the Government has already concluded

data—no one can get in without a password." Steganos, Safe Overview, http://www.steganos.com/us/products/data-security/safe/overview (last visited Feb. 15, 2010).

[67] *Pearson*, 2006 U.S. Dist. LEXIS 32982, at *13. Privacy advocates will presumably cry foul here: why should relatively large, encrypted files warrant an inference of guilt? Indeed, the government sought to introduce "evidence that various files on computer media, including a 2.3 gigabyte file on an external hard drive, are encrypted, as *consciousness of guilt*." *Id.* at *42 n.4 (emphasis added). Surely encryption is not probative of guilt independent of the content encrypted. In fairness, the government also sought to introduce "any sexually explicit images of minors involved (in the event they are located on the encrypted computer media), as direct evidence of reacquiring and receiving the images." *Id.* Absent this "direct evidence," however, dangling encrypted files (of unknown content) before the jury would merely bait the defendant into proffering an innocent explanation, lest the jury infer an incriminating one. Such a dilemma surely lies at the very core of any right to silence. *See id.*

[68] *Id.* at *13-*14.

[69] *Id.* at *3.

[70] *Id.* at *52.

[71] *Id.* at *53-54.

[72] *Id.* at *54.

[73] *Id.* at *53 (citing Fisher v. United States, 425 U.S. 391, 409 (1976)).

[74] *Id.* at *54.

[75] *Id.*

> upon forensic examination that they are encrypted. The Government has also rightfully obtained information from Defendant indicating that he intended to encrypt certain files, and that Defendant was provided with encryption software. Thus, the existence and use of encryption software on the files recovered from Defendant is all but a for[e]gone conclusion, and knowledge of the actual password adds little to what the Government already knows in this regard.[76]

Given these circumstances, the court found that the government had met its burden under the first prong of the Circuit's test: the government had described with reasonable particularity the location of certain files known to exist.[77]

Unfortunately, an unusual complication muddled the court's analysis under the second prong. The defendant's father, whose computer the government had seized, rather belatedly claimed to represent the defendant as his attorney.[78] Though contrary to the evidence, he further asserted that his legal relationship with the defendant had commenced before the confiscation, thus rendering the relevant documents immune from subpoena by the attorney-client privilege and work-product doctrine.[79] With this new twist, the court labored to unravel the authentication issue in the face of conflicting affidavits made by the defendant.[80] On the one hand, he had "already voluntarily asserted under oath that the seized files contain[ed] *his* material."[81] On the other hand, he claimed that an attorney, namely his father, had prepared at least some of the confiscated documents.[82] Conceivably then, the defendant lacked ownership or control over some parts of the encrypted hard drive.[83] From this tangle of proof and privilege, the court teased out the evidentiary implication: "[P]roduction of the password would provide powerful evidence on the issue of authentication of the encrypted files that his father did not produce because it would provide a link in the chain of ownership and control of any incriminating encrypted files."[84] In light of this finding, the district court scheduled a pretrial hearing to determine whether the government could authenticate the encrypted files by means other

[76] *Id.* at *58-59.

[77] *Id.* at *57; *see In re* Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992, 1 F.3d 87, 93 (2d Cir. 1993) (stating that, under *Fisher*, incriminating testimony results only "if the existence and location of the subpoenaed papers are unknown to the government.").

[78] *Pearson*, 2006 U.S. Dist. LEXIS 32982, at *8-*9, *14.

[79] *Id.* at *20-*21.

[80] *Id.* at *24-*25.

[81] *Id.* at *60 (citations to the record omitted).

[82] *Id.* at *21.

[83] *See* Hoffman v. United States, 341 U.S. 479, 486 (1951) (establishing the "link in the chain of evidence" rule).

[84] *Pearson*, 2006 U.S. Dist. LEXIS 32982, at *62 (citing *Hoffman*, 341 U.S. at 486).

than compelled production of the password.[85] Pending the outcome of this hearing, the court reserved judgment on defendant's motion to quash the subpoena.[86]

The decision in this complex case faithfully comports with both *Fisher* and *In re Grand Jury Subpoena*: where the government can independently authenticate documents known to exist in a particular location, the Fifth Amendment will not protect them from an otherwise valid subpoena. However, the parties apparently did not raise—and the court did not discuss—the issue of whether this rule should apply to encrypted documents. This Note presents the uneasy case for why encrypted documents warrant special consideration.[87]

### 2. Existence and Location

In *Boucher*, an even more recent decision from the Second Circuit, the court focused its attention on the first prong of the *In re Grand Jury Subpoena* test.[88] In that case, the defendant had sought to enter the United States from Canada, when a U.S. Customs and Border Protection inspector searched his laptop computer and found approximately forty thousand images, at least some of which had file names clearly indicative of child exploitation.[89] Further inspection by a Special Agent for Immigration and Customs Enforcement (ICE) revealed pornographic images of both children and adults.[90] Boucher admitted that sometimes, while searching for the latter, he

[85] *Id.* at *62.

[86] *Id.* at 63. This partial victory failed to exculpate Pearson, however, who subsequently pled guilty to multiple counts of producing, transporting, receiving, and possessing child pornography. United States v. Pearson, 570 F.3d 480 (2d Cir. 2009). Although the Second Circuit vacated an order to pay restitution in the amount of $974,902 to one of the victims, and again remanded the case for this limited purpose, the appellate court otherwise upheld the district court's conviction and sentencing. *Id.*

[87] *See infra* Parts II and III.

[88] *In re* Grand Jury Subpoena to Sebastian Boucher, 2009 U.S. Dist. LEXIS 13006 (D. Vt., Feb. 19, 2009).

[89] While *Pearson* and *Boucher* both dealt with child pornography, the definition of "contraband" includes all manner of illicit material: "1. Illegal or prohibited trade; smuggling. 2. Goods that are unlawful to import, export, or possess." BLACK'S LAW DICTIONARY 341 (8th ed. 2004). Whether a statute banning possession of videos depicting animal cruelty unconstitutionally limits speech has recently drawn the attention of the Supreme Court. *See* United States v. Stevens, 533 F.3d 218 (3d Cir. 2008), *cert. granted*, 129 S. Ct. 1984 (U.S. April 20, 2009) (No. 08-769); *see also* Krista Gesaman, *Kitty Stomping is Sick*, NEWSWEEK, October 3, 2009, *available at* http://www.newsweek.com/id/216740 (questioning whether images of animal cruelty are equivalent to child pornography).

[90] *In re* Grand Jury Subpoena to Sebastian Boucher, No. 2:06-mj-91, 2009 U.S. Dist. LEXIS 13006, at *4-*5 (D. Vt. Feb. 19, 2009)

unknowingly downloaded the former, but claimed to have deleted such images when he realized their content.[91]

Upon request, the defendant voluntarily opened the computer's Z drive, which the special agent had unsuccessfully attempted to access.[92] Determining that these images met the definition of child pornography, the special agent arrested Boucher and shut down the laptop.[93] Subsequently, the government could neither find nor open the Z drive, which had encrypted automatically and required a password to recover.[94]

On Fifth Amendment grounds, a magistrate judge granted defendant's motion to quash a grand jury subpoena directing him to provide this password.[95] Under de novo review, however, the district court judge rejected the magistrate's order and denied the motion to quash.[96] As in *Pearson*, the *Boucher* court quickly quelled any contention that the substance of the encrypted material might warrant shielding under the Self-Incrimination Clause: "There is no question that the contents of the laptop were voluntarily prepared or compiled and are not testimonial, and therefore do not enjoy Fifth Amendment protection."[97]

Whereas the magistrate had deemed the "foregone conclusion" rationale inapplicable because the government had viewed only a small portion of the Z drive (and hence could not know whether most of the files contained incriminating materials or not), the district court rejected this reasoning: "Second Circuit precedent . . . does not require that the government be aware of the *contents* of the files; it requires the government to demonstrate 'with reasonable particularity that it knows of the existence and location of subpoenaed documents.'"[98]

While denying the motion to quash, the district court forbade the government from exploiting defendant's compliance with the

[91] *Id.* at *5.

[92] *Id.*

[93] *Id.*

[94] To avoid this problem, law enforcement officers are often trained not to shut down any computer equipment seized without expert assistance. Similarly, many law enforcement agencies, as a matter of policy, attempt to serve search warrants on a suspected pedophile when child pornography is likely to be contemporaneously displayed on his computer screen—thus circumventing the encryption problem entirely. *See* Identifying Online Child Exploitation Crimes, *supra* note 1.

[95] The government later clarified that production of an unencrypted version of the Z drive, in lieu of the password, would also suffice. *See Boucher*, 2009 U.S. Dist. LEXIS 13006, at *6.

[96] *Id.* at *10-*11.

[97] *Id.* (citing *Fisher* at 409-10 and United States v. Doe, 465 U.S. 605, 611-12 (1984) ).

[98] *Id.* at *8 (quoting *In re* Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992, 1 F.3d 87, 93 (2d Cir. 1993)).

subpoena to authenticate the unencrypted files before a jury.[99] The district court certainly found persuasive—perhaps even dispositive—the defendant's incriminating cooperation,[100] the absence of which might well have affected the outcome:

> Boucher accessed the Z drive of his laptop at the ICE agent's request. The ICE agent viewed the contents of some of the Z drive's files, and ascertained that they may consist of images or videos of child pornography. The government thus knows of the existence and location of the Z drive and its files.[101]

Moreover, because Boucher had already admitted to possessing the computer, and previously provided the ICE agent with Z drive access, the government assured the court that sufficient evidence tied the defendant to the encrypted files—even without his compelled act of production.[102] As in *Pearson*, the court in *Boucher* followed the precedents set out by the Supreme Court in *Fisher* and the Second Circuit in *In re Grand Jury Subpoena*, but without considering whether encrypted documents logically lie within the scope of the holdings of those cases. The nature of encryption suggests that encoded documents at least warrant a different analysis—if not a different result. An appreciation for why courts ought to afford encryption special attention requires a basic familiarity with the underlying technology.

## II. ENCRYPTION

### *A. Absolute Privacy*

The concept of secret writing is probably as old as writing itself.[103] The very hallmark of the written word—its permanence—creates a vulnerability for sensitive information.[104] Of course, one

[99] *Id.* at *10.

[100] Similarly, cooperation doomed John Doe, who voluntarily allowed the government to examine the calendar he had doctored. *See In re* Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992, 1 F.3d at 89. Likewise, Pearson undermined his authentication defense when he complained that the government had seized "his" materials. *See Pearson*, 2006 U.S. Dist. LEXIS 32982, at *60.

[101] *Boucher*, 2009 U.S. Dist. LEXIS 13006, at *9.

[102] *Id.* at *10.

[103] Cryptography, as opposed to other forms of secret writing, dates back at least four thousand years to ancient Egypt, where cryptic hieroglyphics decorated the tombs of kings. *See* Fred Cohen & Associates, 2.1 A Short History of Cryptography, http://all.net/books/ip/Chap2-1.html (last visited Feb. 16, 2010).

[104] Misplaced battle plans are an important example. Robert E. Lee's secret instructions for his confederate generals at the Battle of Antietam famously fell into enemy hands, but the cautious union commander, George B. McClellan, characteristically squandered the opportunity.

means of safeguarding an important document is to physically sequester it. This strategy might include hiding the document in a secluded location. The drawback of this approach is that secret hiding places might be difficult for the creator of the document to access as well, thus hindering the his ability to read it again. After all, if future access is completely unimportant, the document might as well be destroyed. This tension between privacy and accessibility has driven the development of codes and ciphers, particularly in the context of warfare.[105]

Ciphers, which encode messages by replacing one set of letters or symbols with another set of letters or symbols, predate modern languages altogether.[106] Caesar sent messages to the battlefront by shifting the alphabet forward by exactly three letters.[107] Upon receipt of the cipher, his generals would simply shift the letters back and read the message.[108] Obviously, the security of this system depended entirely on the secrecy of the method. As the technique became widely known, such a "shifting" cipher could no longer serve its purpose.[109]

Modern cryptographic systems employ a different approach: the method of encryption is often made freely available, and users actually publish "half" of their keys.[110] Such public key encryption

*See* Harvey Craft, *Robert E. Lee's Lost Battle Orders*, SUITE101.COM, Jan. 21, 2010, http://us-civil-war.suite101.com/article.cfm/robert_e_lees_lost_battle_orders.

[105] *Id.*

[106] Ancient civilizations of the Mesopotamia created "atbash" ciphers—wherein the first and last characters of the alphabet are exchanged, the second and second-to-last letters are traded, and so forth (so that ABC becomes ZYX and conversely). *Id.*

[107] Thus, "veni, vidi, vici" ("I came, I saw, I conquered"—attributed to Julius Caesar in 47 B.C.) would become "zmqm, zmgm, zmfm" (in the classical Latin alphabet). *See* Chris Savarese & Brian Hart, Cryptography: The Caesar Cipher, http://starbase.trincoll.edu/~crypto/historical/caesar.html (last visited Feb. 16, 2010).

[108] *Id.*

[109] Of course, an improvement can be made by shifting up (or down) some other number of letters, but an enemy need only try all twenty-two possible shifts (classical Latin had no "j," "u," or "w") to recover the message. Substituting the letters arbitrarily vastly increases the number of possibilities—to a whopping 25,852,016,738,884,976,639,999 for a twenty-three letter alphabet. Yet, given a long enough message, many amateurs can easily solve such puzzles (generally called "cryptograms" in English) by exploiting the frequency of certain letters and the spelling patterns of familiar words. (Try this one: "L fdph, L vdz, L frqtxhuhg."—Mxolxv Fdhvdu.)

[110] *See* RSA Laboratories, What is public-key cryptography?, http://www.rsa.com/rsalabs/node.asp?id=2165 (last visited Feb. 16, 2010) (explaining the basic concept of public key encryption); Prime Number Hide-and-Seek: How the RSA Cipher Works, http://www.muppetlabs.com/~breadbox/txt/rsa.html (last visited Mar. 22, 2010) (basic mathematical introduction to RSA). As the most popular public key encryption system, RSA has stood the test of time. *See* Sara Robinson, *Still Guarding Secrets After Years of Attack, RSA Earns Accolades for Its Founders*, 36 SIAM NEWS 5 (2003), *available at* http://www.msri.org/people/members/sara/articles/rsa.pdf; *see also* Dan Boneh, *Twenty Years of*

systems are analogous to email systems: a user makes his address widely known so that others can send him information, while his password remains secret so that no one but he can read what others have sent.[111] Understanding the paradigm—public addresses coupled with private passwords—does not get an identity thief very far, though, since he knows only that some unknown password will unlock the inbox.[112] If a particular password is compromised, the entire system need not be discarded—the user simply creates a new password.

While the mathematics enabling both cryptography[113] (making codes) and cryptanalysis (breaking them) lie well beyond the scope of this Note,[114] encryption ultimately derives its power from a simple truth, one that any elementary student can readily appreciate: certain arithmetic problems are easy to ask but hard to answer.[115] While computers enable faster solutions, they also engender harder problems.[116] Even as the exponential increase in processing speed

*Attacks on the RSA Cryptosystem*, 46 NOTICES OF THE AMERICAN MATHEMATICAL SOCIETY 202-13 (1999), *available at* http://crypto.stanford.edu/~dabo/papers/RSA-survey.pdf (mathematical overview).

[111] *But see* Tom Van Vleck, The Risks of Electronic Communication, http://www.multicians.org/thvv/emailbad.html (last visited Mar. 22, 2010) (warning that system administrators, software bugs, and security break-ins pose risks to the confidentiality of email).

[112] *See* Tom Van Vleck, The History of Electronic Mail, http://www.multicians.org/thvv/mail-history.html (last visited Mar. 22, 2010) (personal account of the development of many familiar features of electronic communication).

[113] *See generally* Cybernetica Institute of Information Technology, Cryptology Pointers, http://research.cyber.ee/~lipmaa/crypto (last visited Feb. 16, 2010) (collecting and organizing thousands of links to websites related to various aspects of cryptography).

[114] For such a discussion, see Reitinger, *supra* note 3 (citing BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C, 284 n.11 (2d. ed. 1996)).

[115] Many encryption strategies take advantage of certain mathematical operations that, though reversible, are much easier to perform "forwards" than "backwards." *See* W. Diffie & M Hellman, *New Directions in Cryptography*, 22 IEEE TRANSACTIONS ON INFORMATION THEORY 644-54 (discussing "one-way" or "trap-door" functions as applied to public key encryption). Factoring provides a simple yet powerful example. *See generally* Richard Brent, *Recent Progress and Prospects for Integer Factorisation Algorithms*, *in* 1858 LECTURE NOTES IN COMPUTER SCIENCE: PROCEEDINGS OF THE 6TH ANNUAL INTERNATIONAL CONFERENCE ON COMPUTING AND COMBINATORICS 3-22 (2000), *available at* http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.36.6833 (turn-of-the-century evaluation of integer factoring). Some whole numbers—the ones you use to count sheep (as opposed to fractions, negatives, and more exotic quantities)—are the product of smaller (whole) numbers. *See* The Prime Pages, http://primes.utm.edu (last visited Mar. 22, 2010). For example, thirty is the product of six and five, while six is the product of two and three. For this reason, whole numbers like thirty (and six) are called "composites," while the "factors" five, two, and three—which cannot be expressed as products of still smaller whole numbers—are called "primes." *Id.* While multiplying large (prime) numbers together is quite tedious, factoring a large composite number into its unique set of primes is unimaginably more difficult. *See supra* note 3.

[116] Computers facilitate the factoring of enormous composite numbers necessary to crack many encryption systems. *See* Kleinjung et al., *supra* note 3. On the other hand, computers

continues unabated,[117] such anticipated technological improvements pose little threat to robust encryption schemes.[118] Only a staggering revolution in computing power would cast any real doubt on the utility of encryption.[119] Both the promise and peril of encryption arise from its very effectiveness—properly implemented, a strong encryption regime provides near absolute privacy.[120]

### *B. An Appropriate Analogy*

Since the common law often develops by analogy,[121] the similarity—or lack thereof—between encrypted documents and other types of subpoenaed materials must be carefully considered. While the *Pearson* and *Boucher* courts apparently assumed that the private papers doctrine applies to encrypted files,[122] the propriety of this presumption might depend on how encryption is conceptualized.

also aid in constructing a larger modulus from which to construct a stronger encryption system. *Id.*

[117] "Moore's Law" predicted in 1965 that the number of transistors per integrated circuit (a proxy for processing speed) would double every year. *See* Gordon E. Moore, *Cramming More Components onto Integrated Circuits*, ELECTRONICS MAGAZINE, April 19, 1965, *available at* ftp://download.intel.com/museum/Moores_Law/Articles-Press_Releases/Gordon_Moore_1965_Article.pdf. This prediction has proven remarkably accurate through at least 2008. *See also* John Markoff, *After the Transistor, A Leap into the Microcosm*, N.Y. TIMES, Aug. 31, 2009, *available at* http://www.nytimes.com/2009/09/01/science/01trans.html?_r=1&ref=science.

[118] *But see* Kleinjung et al., *supra* note 3 (reporting the successful factorization of a 232-digit number, predicting that factorization of a 1024-bit RSA modulus is entirely possible within the next decade, and warning that 1024-bit RSA encryption should be phased out in the next few years).

[119] In theory, quantum computing would seriously undermine any encryption strategy based on factoring, but the creation of quantum computers have remained elusive. *See* Brent, *supra* note 115, at 2 (citing P.W. Shor, *Polynomial Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, 26 SIAM J. COMPUTING 1484, 1484-1509 (1997), *available at* http://dx.doi.org/10.1137/S0097539795293172).

[120] *See* Reitinger, *supra* note 3, at 171 ("[T]he ability to encrypt information may provide computer users with near absolute privacy for the content of their communications."). Dave Cullinane, Chief Information Security Officer for eBay Marketplaces, has similarly opined: "Encryption is almost certainly the best single solution and probably the ultimate line of defense for protection of sensitive information." PGP, White Paper, PGP Webcast Summary: The Role of Encryption in Data Protection (2007), *available at* http://download.pgp.com/pdfs/whitepapers/PGP-Cullinane-Webcast_WP_070205_F.pdf.

[121] For example, the Copyright Act does not explicitly provide for secondary liability; nevertheleśs, courts have developed the doctrine of vicarious liability by relying upon principles from properly law. *See* Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 261-62 (9th Cir. 1996) (rejecting "landlord-tenant" analogy adopted by district court, where defendant exercised considerable control over "swap meet" featuring sales of counterfeit recordings, and following "dance hall" line of cases: operator of entertainment venue rendered vicariously liable for infringing performances if he (1) controls the premises and (2) obtains direct financial benefit from audience paying to hear it). *Id.* at 261-65.

[122] *See supra* Parts I.C.1 and I.C.2.

### 1. Lost in Translation

If encryption is merely a translation, then a serious problem arises. Under *Fisher*, the state may only subpoena voluntarily created documents.[123] Given a work of any complexity, however, a translation necessarily creates a "new" document.[124] Indeed, critics revere George Chapman's *Iliad* and Alexander Pope's *Odyssey* as much for the translators' English as Homer's Greek.[125] Even setting aside the rhythm and rhyme of poetry, "exact translations" are quite impossible due to the puns, idioms, synonyms, and colloquialisms of everyday speech.[126]

Of course, translating ancient Greek into English differs markedly from encrypting plaintext into ciphertext,[127] for the very reason that two classics scholars would likely translate the same document differently. Encryption precisely preserves all of the original content; that is, encrypting and then decrypting a document results in no loss of information—unlike translation, which necessarily lacks such robustness.[128] For example, if Pope were to translate Chapman's *Iliad* back into ancient Greek, the retranslation would not be mistaken for Homer's original. Indeed, even Chapman could not retranslate Chapman's *Iliad* into the original. Arguably, at least, encryption does not fundamentally alter the message, even though retrieval of a readable form requires more than the naked eye.

[123] Fisher v. United States, 425 U.S. 391, 409 (1976).

[124] *See* Reitinger, *supra* note 3, at 177 ("Translation, at least when performed by a human being, involves the application of human reasoning and communication to a complex problem, and can alter meaning or chance nuances easily.").

[125] *See generally* Editor Eric, Translations of the Iliad, http://www.editoreric.com/greatlit/translations/Iliad.html (last visited Feb. 16, 2010) (comparing a select few of the many hundreds of translations of Homer's masterpiece – including the iconic versions of both Pope and Chapman). John Keats later immortalized the Chapman translation in his eponymous sonnet. John Keats, *On First Looking into Chapman's Homer* (1884), *reprinted in* THE OXFORD BOOK OF ENGLISH VERSE, 634 (Sir Arthur Thomas Quilller-Couch ed., 1919), *available at* http://www.bartleby.com/101/634.html (last visited Feb. 10, 2010). Cryptography purportedly appears in Book VI of the *Iliad*, where Bellerophone carries a secret message ordering his own death. *See* Cohen, *supra* note 103. Translations are themselves cryptic, however. *See, e.g.*, The Project Gutenberg Etext of The Iliad, by Homer, http://www.gutenberg.org/dirs/etext00/iliad10.txt (last visited Feb. 10, 2010) (translation by Samuel Butler, which speaks only of "lying letters of introduction, written on a folded tablet").

[126] *See* BILL BRYSON, THE MOTHER TONGUE: ENGLISH AND HOW IT GOT THAT WAY (Perennial 1990).

[127] "Plaintext" refers to unencrypted or decrypted text; encrypted text is called "ciphertext."

[128] *See* Reitinger, *supra* note 3, at 177 ("Encryption [as contrasted with translation] is a purely mechanistic process that does not of necessity add, subtract, or alter information.")

After all, virtually any magnetic or electronic storage device—be it microfiche or a Macintosh—entails modern technology to obtain usable data. Even a printed document requires light to be read. It would strain credulity to suggest that placing a document in a dark room even temporarily alters its content. Though the message is not currently perceivable, the flip of a switch immediately restores its readability without any change to the document itself. As with other storage technologies, from cassette tapes to flash drives, modern encryption derives much of its utility from the ease with which a properly equipped user can recover the original message.

### 2. Safe But Not Sound

Because translation provides a poor parallel, a different analogy may be more apropos. Many commentators have likened encryption to placing documents in a locked safe.[129] Indeed, this simple comparison does capture an important functional aspect of encrypted documents: with the right key, anyone can gain access, but otherwise, recovery is extremely difficult and requires brute force. While strong encryption provides virtually impenetrable protection, an unauthorized user could theoretically gain access with exhaustive effort,[130] much like a burglar might attempt to defeat a wall safe by trying all of the innumerable combinations. On the other hand, if the anticipated time needed for a lucky guess exceeds the burglar's lifetime, the stored documents would remain quite secure.

In some ways, then, the safe analogy does provide a useful comparison to encryption, but significant dissimilarities may lead to confusion. For example, an encrypted file is easy to delete without opening, while the contents of a bank vault are virtually impossible to destroy without first achieving access. More importantly, the contents within a safe remain invariant—locking and unlocking the door does not change the documents within. Encryption though, does change—rather dramatically—the manifestation of the plaintext: thus "veni, vidi, vici" becomes "zmqm, zmgm, zmfm."[131]

While a safe suggests physical sequestering, an encrypted message could be published in the newspaper while still retaining the same level of protection. Rather than sending a cipher, Caesar could have placed his military instructions in a strongbox and had a legion of soldiers march it to the front lines. The former technique uses

[129] *See supra* note 66.

[130] *See supra* note 3.

[131] *See supra* note 107.

encryption; the latter does not. This example illustrates a key feature of encryption not shared by physical seclusion—the relative ease with which secret information can be communicated. Over the Internet, encrypted documents are easily transferred surreptitiously, while delivering a wall safe would indeed require a small army. Such shortcomings suggest that analyzing encryption by analogy to a safe might be less than sound.[132]

### 3. Shredding the Safe Analogy

If encryption were truly analogous to locking documents in a safe, then encrypted files should be treated like any other subpoenaed materials. Placing papers in a safe cannot lawfully preclude a grand jury from reading them any more than filing them in an unlocked cabinet or saving them on a digital storage device.[133] Of course, the government must clear the *Fisher* hurdles regarding existence, location, and authentication;[134] a grand jury cannot compel the opening of a safe on the off chance that relevant documents might be found inside, but neither can it require the opening of an unlocked desk drawer on the same pretense.[135] If encryption involves nothing more than sequestering otherwise discoverable evidence, then ciphertext indeed falls squarely within the private papers doctrine.

As indicated above, however, the safe analogy fails to capture the essence of encryption. Unlike a steel briefcase, ciphertext thwarts an unauthorized interceptor due to the inherent state of the message, not because of an outer casing. Due largely to the ambiguity of

[132] Neither the *Pearson* nor *Boucher* courts explicitly analogized encryption as a safe. However, Pearson himself did characterize his files in this way—as did the company from which he obtained the encryption software. *See supra* notes 63-66 and accompanying text. Indeed, many data security companies liken their encryption software to a safe or vault. *Id.* As this analogy permeates the industry, courts are likely to adopt it—explicitly or otherwise—and the features, including the defects, of the analogy might color the common law. *Id.*

[133] *In re* Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992, 1 F.3d at 93 ("Production may not be refused 'if the government can demonstrate with reasonable particularity that it knows of the existence and location of subpoenaed documents.'") (quoting United States v. Fox, 721 F.2d 32, 36 (2d Cir. 1983)).

[134] Fisher v. United States, 425 U.S. 391, 409 (1976) ("Compliance with the subpoena tacitly concedes the existence of the papers demanded and their possession or control by the taxpayer. It also would indicate the taxpayer's belief that the papers are those described in the subpoena.").

[135] *In re* Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992, 1 F.3d at 93 ("While the contents of voluntarily prepared documents are not privileged, the act of producing them in response to a subpoena may require incriminating testimony . . . 'if the existence and location of the subpoenaed papers are unknown to the government.') (quoting United States v. Fox, 721 F.2d 32, 36 (2d Cir. 1983)).

languages, the translation analogy must be discarded,[136] but it at least distinguishes the original document from the resulting ciphertext. While the message or meaning of the text before and after encoding may endure, the physical state of the document does not. The data "scrambling" that encryption effectuates should challenge the apparent assumption of courts and commentators alike who treat compulsory decryption of previously encrypted material as voluntarily created. The following thought experiment, although still imperfect, may provide a meaningful improvement.

Imagine a burglar learns that important documents are stored in a safe. To his surprise he finds the door unlocked. Upon removing the papers however, he is dismayed to find that what had been standard sheets of paper have been shredded into a thousand tiny shards. On the back of each little sliver is a unique number from one to one thousand. Alas, placing the scraps in numerical order reveals no discernable message. While an appropriate ordering does exist, only the person who shredded the document knows which of the unimaginably many combinations unscrambles the code. Out of disgust, the burglar might destroy the document or he might go ahead and steal it, but he could not actually read it anytime soon.

This analogy captures several hallmarks of encryption. First, such a mutilated document is quite unreadable in such a state. Second, though exceedingly difficult, this kind of destruction lends itself to complete restoration and future accessibility in a way that burning it to ashes, for example, does not. Third, reconstruction of the document requires no interpretation—an extremely tedious but mechanistic application of the cipher would suffice. Fourth, transmitting the message from sender to receiver requires no more effort than conveyance of the original. Fifth, while the code could be broken, either by chance or exhaustive effort, knowledge of the key would hasten decryption by several orders of magnitude.[137] Finally, the shredded document is not a copy of the original—it *is* the original. All the bits that comprised the original still exist, and no others have been created in the process.

Would unscrambling the bits create a new document? Could the government compel that creation? The answers to these questions might—but probably should not—depend on the nature of the encrypted documents.

[136] *See supra* Part II.B.1.

[137] *See supra* note 3.

## III. COMMON LAW VERSUS COMMON SENSE

### A. Ciphertext as "Private Papers"

The terms "plaintext" and "ciphertext" make sense when the document to be encrypted actually and exclusively contains text. If Julius Caesar needed to send a secret message—"Et tu, Brute?"—he could employ his eponymous cipher,[138] but if he wished to include a picture of Brutus, he would be out of luck. Since any digital medium is ultimately a long string of ones and zeros,[139] however, encrypting image or audio files is conceptually indistinguishable from encoding actual text. Arguably, then, the law should treat all encrypted documents uniformly, without regard to their content. At the very least, in the interest of public policy, when audiovisual files consist solely of pure contraband, the law should afford them no greater protection than conventional private papers—and perhaps even less.

First, though, a word on "plaintext" qua text. Under the rubric of a translation analogy, the Fifth Amendment would clearly preclude the decryption of encrypted textual files, because responding to a subpoena would entail the creation of new documents in contravention of the *Fisher* requirement that only voluntarily created writings are subject to compulsory production before a grand jury.[140] Assuming, however, that the document warrants no protection, in spite of its private nature, before encryption, it makes little sense to deprive the grand jury of relevant evidence, after the encoding, merely because the author has transformed it into an even more private form. Once the government and the judiciary have decided that the potential probative value entitles a grand jury to examine a document, what rationale can justify its seclusion on account of the author having taken pains to sequester it? The purely mechanistic nature of encryption and decryption weighs against tolerating such a defense. Certainly, if the author can, with minimal effort, produce the subpoenaed document in readable form, exactly as he had written it, such action can hardly be construed as compelling the defendant to be a "witness against himself."[141] If the law is otherwise, then either the law should be changed or the analogy discarded. As noted above, many reasons support the latter approach.[142]

[138] *See supra* note 107 and accompanying text.

[139] *See* Representing Binary Quantities, http://www.eelab.usyd.edu.au/digital_tutorial/chapter1/1_4.html (last visited Mar. 22, 2010).

[140] *See supra* notes 31-35 and accompanying text.

[141] U.S. CONST. amend. V.

[142] *See supra* Part II.B.3.

As contended above, the prototypical safe should be replaced with the shredder analogy. Whichever metaphor is decided upon, however, the outcome should remain the same: taking pains to hide discoverable evidence should not augment its legal protection. Moreover, the reconstruction of extant shards, though transformative, cannot plausibly be considered a new document for purposes of the Fifth Amendment. The document has always existed, though the message had been temporarily garbled in its encrypted state. That the defendant, rather than the government, can quickly obtain a readable version of the document should not render it immune from subpoena. Most documents, especially electronically-stored information, can be compiled more easily by their possessor than by any other person. Hence, in a civil case, the parties bear the burden of producing their own documents for the sake of efficiency.[143] That encryption makes for an especially stark disparity—the government would require years to obtain the plaintext while the defendant could decode the ciphertext in a matter of seconds—weighs in favor of discoverability and not against it. Absent exceptionally strong countervailing privacy interests, encryption should not obstruct the truth-seeking function of both grand and petit juries.

### *B. The Square Peg of Contraband*

At least in the case of pure contraband, a fundamental problem arises in conceptualizing encryption as a reversible shredding process instead of the proverbial safe. Another thought experiment illustrates the underlying difficulty. Imagine the world's most accomplished bomb maker, Mr. Bombardier, has just finished his latest creation—a particularly complex, intricate, and fragile explosive—when the police burst into his workshop. A lesser bomb maker would probably place the device in a safe, if one were available, but doing so could hardly protect it from a subpoena. By blowtorch, if necessary, the government could open the safe and recover the bomb.

Fortunately for Mr. Bombardier, a very clever craftsman indeed, this bomb contains a "self-de*con*struct" button. Rather than exploding when depressed, the bomb merely flies apart into its myriad components. While circumstantial evidence may suggest that the assorted parts had once constituted an explosive, in no sense can the various screws and wires be considered a bomb now. Suppose that, with years of effort, an explosives expert might be able to reconstruct

[143] FED. R. CIV. P. 26.

the bomb, while Mr. Bombardier himself could definitely rebuild it—and much more quickly.

Presumably, no trial court would compel Mr. Bombardier to reconstitute into contraband sundry components that, in their current state, are unrecognizable as such.[144] Could a court compel him to tell government explosive experts how to rebuild the bomb? Surely any such instructions lie squarely within the category of compelled, incriminating testimony that the Fifth Amendment precludes.[145] Though a bit pinched, this hypothetical nevertheless suggests a disquieting thought: perhaps the Self-Incrimination Clause actually prevents the government from demanding the decryption of encrypted contraband, such as child pornography—even when its existence and location are known to the government and can be independently authenticated.

Encryption presents difficulties precisely because its uniqueness renders it incomparable to more familiar kinds of evidence. Rarely, if ever, can the defendant—but not the government—reconstitute "destroyed" evidence already seized by the state. Of course, when criminal suspects attempt to destroy or conceal evidence, the government may endeavor to find or reconstruct it. Thus, a drug dealer who dissolves illicit powder in water has not really destroyed the evidence, since recovery of the solute is the stuff of middle school science experiments, but neither does the government require any special knowledge on his part to recover the contraband. Moreover, the government generally obtains contraband by seizing it—with or without a warrant. Where a grand jury demands production of an unencrypted copy of an encrypted file thought to contain contraband (as opposed to the key with which to decrypt it), the government does nothing less than subpoena contraband. Such a procedure is a huge departure from the "mere evidence" rule of *Gouled* that prohibited the government from seizing private papers (even with a warrant) from the house of a person solely for the purpose of collecting incriminating evidence against the owner.[146] If the law allows the government to subpoena such materials, it underscores the

[144] *See* Doe v. United States, 487 U.S. 201, 211 ("It is the 'extortion of information from the accused,' *Couch v. United States*, 409 U.S. 322, 328 (1973), the attempt to force him 'to disclose the contents of his own mind,' *Curcio v. United States*, 354 U.S. 118, 128 (1957), that implicates the Self-Incrimination Clause."); Id. at 220 ("If John Doe can be compelled to use his mind to assist the Government in developing its case, I think he will be forced 'to be a witness against himself.'") (Stevens, J., dissenting).

[145] *See* Doe v. United States, 487 U.S. 201, 212 (1988) ("Historically, the privilege was intended to prevent the use of legal compulsion to extract from the accused a sworn communication of facts which would incriminate him.")

[146] *Gould v. United States*, 255 U.S. 298, 309 (1921); *see supra* note 25.

enormous erosion in Fifth Amendment protection that has occurred over the last century, at least as applied to private papers.[147]

Yet, allowing the Fifth Amendment to thwart the disclosure of pure contraband, while diaries and datebooks enjoy no such protection,[148] defies common sense. Whether or not genuinely private writings should enjoy greater Fifth Amendment protection than current precedent recognizes, affording additional protection to pure contraband—particularly such invidious material as child pornography—surely contravenes public policy. This Note does not suggest otherwise; it merely acknowledges the "tyranny of small decisions" that characterizes common law development.[149] Application of the private papers doctrine to encrypted contraband might be logical, but the Self-Incrimination Clause has drifted far from its original mooring in *Entick* where the contraband seized by the government consisted of seditious papers.[150]

Rather than blindly applying the private papers doctrine to every private document that could conceivably be transcribed to paper, courts would be wiser to clear out the undergrowth beneath an increasingly arcane Fifth Amendment jurisprudence.[151] Absent Supreme Court guidance however, such pruning can scarcely occur at the ground level of trial courts, which must apply the law—not improve it.[152] Ubiquitous encryption lies just beyond the horizon, and

[147] *See supra* Part I.A.

[148] See, e.g., *In re* Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992, 1 F.3d 87, 90 (2d Cir. 1993).

[149] A.E. Kahn, *The Tyranny of Small Decisions*, 101 KYKLOS 23, 23-46 (1966), *available at* http://opus1journal.org/articles/article.asp?docID=140 ("Decisions that are small in size, time perspective, and in relation to their cumulative effect may lead to suboptimal resource allocation.").

[150] Entick v. Carrington, [1765] 95 Eng. Rep. 807 (K.B.)

[151] A partial list of compelled, incriminating acts deemed non-testimonial by the Court—and hence beyond the scope of Fifth Amendment privilege—suggests that the exceptions have swallowed the rule. *See* Baltimore City Dept. of Social Servs. v. Bouknight 493 U.S. 549 (1990) (producing child); Doe v. United States, 487 U.S. 201, 212 (1988) (authorizing disclosure of bank records); California v. Byers, 402 U.S. 424 (1971) (reporting accident); Gilbert v. California, 388 U.S. 263 (1967) (providing handwriting exemplar); United States v. Wade, 388 U.S. 218 (1967) (providing voice recording); Schmerber v. California, 384 U.S. 757 (1966) (providing blood sample); Shapiro v. United States, 335 U.S. 1 (1948) (maintaining required records); United States v. Sullivan, 274 U.S. 259 (1927) (filing income tax return); Holt v. United States 218 U.S. 245 (1910) (put on shirt). Indeed, "the privilege against self-incrimination" no longer accurately describes that Constitutional provision. *See* United States v. Hubbell, 530 U.S. 27, 34 (2000) ("The term 'privilege against self-incrimination' is not an entirely accurate description of a person's constitutional protection against being 'compelled in any criminal case to be a witness against himself.')

[152] Even while advocating in support of ratifying the pending Constitution, by quelling concerns that the proposed judiciary would exercise undue power over legislative bodies, "Publius" acknowledged, nevertheless, the imperative of judicial restraint. *See* THE FEDERALIST

it portends a gathering storm for law enforcement agents—the confluence of near absolute privacy with profligate dissemination. As the utility and availability of encryption technologies inevitably advance, so too must the law.

## IV. CONCLUSION

As both the use and utility of encryption increase, the dilemma faced by law enforcement agencies in *Pearson* and *Boucher* will become more common: the government, having lawfully seized encrypted contraband, will find itself unable to admit the files into evidence—not because of the exclusionary rule, but due to the technical difficulty of decoding ciphertext without the key. While defendants with much to hide might well choose contempt over compliance, the law ought to at least afford prosecutors the legal right to subpoena either the decrypted copy or the password enabling that decryption. The limited case law on point, all from federal district courts in the Second Circuit, appears to comport with this policy objective, subject to the restrictions of *Fisher* and subsequent Second Circuit precedent: the government must prove the existence and location of the subpoenaed documents and possess independent evidence, other than compliance with the court order, for authenticating them.[153]

While the law may thus appear to adequately safeguard the interest of law enforcement in fighting the bundle of child pornography crimes that encryption greatly facilitates, enterprising lawyers can surely craft colorable arguments that encrypted documents should lie outside of the private papers doctrine altogether. Of course, whether that would open to door for greater, rather than less, Fifth Amendment protection remains to be seen. In any event, courts should recognize that the unique nature of encrypted documents at least warrants an independent analysis distinct from other private papers. The current rationale for not distinguishing

NO. 82 (Alexander Hamilton) ("The courts must declare the sense of the law; and if they should be disposed to exercise WILL instead of JUDGMENT, the consequences would . . . be the substitution of their pleasure to that of the legislative body."); *Cf.* Marbury v. Madison, 5 U.S. (1 Cranch) 137, 177 (1803) ("It is emphatically the province and duty of the judicial department to say what the law is. Those who apply the rule to particular cases, must of necessity expound and interpret that rule.") (Marshall, C.J.)

[153] *Compare In re* Grand Jury Subpoena to Sebastian Boucher, No. 2:06-mj-91, 2009 U.S. Dist. LEXIS 13006, at *9-*10, (D. Vt. Feb. 19, 2009), *and* United States v. Pearson, No. 1:04-CR-340, 2006 U.S. Dist. LEXIS 32982, at *58-*59, *62, (N.D.N.Y. May 24, 2006), *aff'd*, 570 F.3d 480 (2d Cir. 2009), *with* Fisher v. United States, 425 U.S. 391, 411-413 (1976), *and In re* Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992, 1 F.3d 87, 93 (2d Cir. 1993).

between unencrypted and encrypted files appears to be an implicit assumption that the latter are not meaningfully different from the former when stored electronically. The *Boucher* and *Pearson* courts might also have likened encryption of documents to their placement in a locked safe, as many security companies and commentators have so analogized.

The day may soon arrive when an adequately briefed court will recognize the deficiencies of this simple comparison, which will call into doubt the previous decisions implicitly premised upon it. This Note has proposed an alternative analogy that, while still imperfect, may provide a better foundation upon which to construct a more satisfying theory. Conceptualizing an encrypted document as having been shredded into myriad pieces, and those pieces labeled with a unique sequence known only to the encoder, captures several important features of encryption. In particular, the original message, while currently unreadable, has been preserved in a very real sense, and can be reconstituted in every detail through purely mechanistic means. This analysis weighs in favors of treating encrypted documents the same as other private papers—essentially preserving the status quo, with the possible exception of encrypted contraband.

Contraband might be more problematic because forcing defendants to reconstitute into contraband material currently unrecognizable as such seems counterintuitive and unprecedented. Compelling defendants to assist the government in perceiving confiscated materials, which will then facilitate their conviction—while unusual, and perhaps unsavory—nevertheless compares favorably to the alternative: effectively granting encrypted contraband greater Fifth Amendment protection than that currently afforded genuinely private writings such as diaries. Whether or not encrypted documents constitute contraband, public policy weighs against further constraints—beyond those of *Fisher*—on the subpoena power of grand juries.

*Nathan K. McGregor*[*]

[*] J.D. Candidate, Vanderbilt University Law School, 2011; Ph.D., Systems Science and Mathematics, Washington University in St. Louis, 2007; B.S., Mathematics/Medieval Studies, University of Notre Dame, 1999. The author would like to thank his wife for her constant support and enduring patience. He would also like to the thank the editorial staff at the *Vanderbilt Journal of Entertainment and Technology Law*, especially Steven Reilly, Megan Bibb, and Brian Van Wyk, whose thoughtful editing substantially improved this Note.