

The Key Theory: Authenticating Decrypted Information in Litigation While Protecting Sensitive Sources and Methods

Nicholas J. Patterson*

Introduction

Since at least the beginning of the Cold War, the U.S. government has grappled with the difficulty of introducing deciphered encrypted information in litigation without exposing sensitive sources and methods. This Article describes a method for cutting that Gordian knot.¹

Encryption has been used since ancient times by militaries, spies, and others to communicate information covertly.² As encryption technology has evolved in complexity and decreased in expense with the advent of computer encryption, it has created new opportunities for foreign powers, foreign and corporate spies, terrorist groups, and criminals.³

* J.D., The University of Chicago Law School; M.Phil., Cambridge University; A.B., The University of Chicago. Counsel for National Security Law and Policy, National Security Division, United States Department of Justice. I greatly appreciate the help of the individuals listed below. I bear sole responsibility for any errors herein. For reading and commenting on drafts of this Article, I thank Matthew A. Anzaldi, Susan Kelley Koeppen, Alexander K. Haas, Philip Hamburger, Orin S. Kerr, Steven P. Lehotsky, Paul Ohm, Eric Posner, Dakota Rudesill, and Benjamin Wittes. For inviting me to the Texas Law Review Symposium and asking me to write this Article, I thank Robert Chesney and the Editorial Board of the Texas Law Review. For suggesting the subject of this Article, I thank Leonard Bailey. For providing assistance concerning the record in the *Wasp Network Case*, I thank Caroline Heck Miller. For providing advice and suggestions regarding Senator Daniel Patrick Moynihan's Commission on Protecting and Reducing Government Secrecy and the Venona project, I thank Mark A. Bradley. The views expressed in this Article are the author's alone and do not represent the position of the United States Department of Justice.

1. The term *Gordian knot* refers to "an intricate problem" and is derived from "a knot tied by Gordius, king of Phrygia, held to be capable of being untied only by the future ruler of Asia, and cut by Alexander the Great with his sword." MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 540 (11th ed. 2003). Interestingly, the Gordian knot itself may have been a cipher. See ROBERT GRAVES, THE GREEK MYTHS § 83.4 (1960) (explaining that the knot may have symbolized the ineffable name of Dionysus which, enknotted like a cipher, would have been passed on through generations of priests and revealed only to the kings of Phrygia).

2. See Brendan M. Palfreyman, Note, *Lessons from the British and American Approaches to Compelled Decryption*, 75 BROOK. L. REV. 345, 349–50 (2009) (describing historical uses of cryptography and the development of cryptography over time).

3. See, e.g., *The Security and Freedom Through Encryption (SAFE) Act: Hearing on H.R. 850 Before the H. Permanent Select Comm. on Intelligence*, 106th Cong. (1999) (statement of Janet Reno, Att'y Gen. of the United States), available at <http://www.justice.gov/archive/ag/testimony/1999/agintell071499.htm> ("[I]t will become far more difficult for the FBI, DEA, and other federal, state, and local, law enforcement agencies, faced with the rising threat from the criminal use of commercially available encryption, to protect the public from crimes such as terrorism, narcotics trafficking, economic fraud, and child pornography."); Palfreyman, *supra* note

This Article articulates a “Key Theory” method for introducing evidence derived from encrypted information while protecting the U.S. government’s sources and methods. Under the Key Theory, if the government were to introduce encrypted information with an unbroken chain of custody or as a record of a regularly conducted activity and provide a key or password in court that deciphers the information, the government would not have to explain how or where it obtained the key or password or how the key or password works. Rather, the government would only have to show that the key or password works to decrypt the information.

This Article articulates a theory to introduce evidence derived from encrypted information where the government has made the judgment to reveal that it can decrypt that information.⁴ Part I provides an overview of the history of encryption, explains the basics of how it works, and shows how it has both grown more difficult to decipher and easier for more people to encrypt with the advent of computer encryption. Part II discusses how protecting sources and methods has historically been a problem when introducing deciphered information as evidence in national security cases. As an example, this Article examines the Federal Bureau of Investigation’s (FBI) decision not to use the information deciphered from the Venona program’s Soviet wire transmissions in espionage prosecutions in the 1950s. Part III explains how evidence is authenticated in the U.S. legal system. Part IV details the legal reasoning behind the Key Theory and shows how a similar approach was applied in the *Wasp Network Case*.⁵ Part V considers arguments defendants may raise against the application of the Key Theory—including Sixth Amendment Confrontation Clause, *Brady*,⁶ and Jencks Act⁷ arguments—and explains why these arguments fail. Part VI describes how the Key Theory can also be used by litigants in civil litigation.

I. The History of Encryption and the Growth of Computer Encryption

Cryptography is “the enciphering and deciphering of messages in secret code or cipher.”⁸ To keep information secret, an individual will encrypt the information and make it unintelligible to unauthorized parties.⁹ An authorized party will decrypt or decipher an encrypted message to read the

2, at 350 (“Today, electronic encryption has become standard practice for governments, corporations, and, to a somewhat lesser extent, individuals.”).

4. As a threshold issue, the government has to make a determination whether it is willing to make public the fact that it has acquired and decrypted the information. There may be instances where the government determines that security considerations prevent it from revealing that it possesses the ability to acquire and decrypt and, therefore, that it will not use the Key Theory in litigation.

5. *United States v. Hernandez*, No. 98-0721-CR-JAL (S.D. Fla. 2001).

6. *Brady v. Maryland*, 373 U.S. 83 (1963).

7. 18 U.S.C. § 3500 (2006).

8. MERRIAM-WEBSTER’S COLLEGIATE DICTIONARY, *supra* note 1, at 302.

9. Palfreyman, *supra* note 2, at 348.

hidden information.¹⁰ Encrypted text is referred to by cryptographers as “ciphertext,” and unencrypted or decrypted text is referred to as “plaintext.”¹¹

Governments, militaries, and individuals have used cryptography to safeguard information and communications throughout history.¹² The ancient Greeks used a primitive form of cryptography. Herodotus describes an individual having his shaved skull tattooed with a secret message and then, after his hair grew back, being sent to the recipient of the message, who had the messenger’s head shaved to reveal the message.¹³ In ancient Rome, Julius Caesar employed a more advanced method of cryptography—he employed the process of shifting every letter in the alphabet up three steps.¹⁴

Since ancient Greek and Roman times, encryption has evolved from simple to increasingly intricate ciphers—such as Napoleon Bonaparte’s Great Paris Cipher¹⁵—to complex mechanical devices—such as the Enigma machine used by Germany in World War II¹⁶ and one-time pads used by the Soviet Union¹⁷—to digital encryption of electronic data.

Currently, electronic encryption is regularly used by governments, corporations, and some individuals to protect information that is either in electronic storage or electronically transmitted.¹⁸ Due to the limits of current

10. *Id.* at 348–49.

11. Phillip R. Reitinger, *Compelled Production of Plaintext and Keys*, 1996 U. CHI. LEGAL F. 171, 172 n.8.

12. Palfreyman, *supra* note 2, at 349.

13. 3 HERODOTUS, *THE HISTORY OF HERODOTUS* 198 (George Rawlinson trans., New York, D. Appleton & Co. 1866).

14. Adam C. Bonin, Comment, *Protecting Protection: First and Fifth Amendment Challenges to Cryptography Regulation*, 1996 U. CHI. LEGAL F. 495, 497 (1996).

15. Napoleon Bonaparte’s Great Paris Cipher contained approximately 1,400 coded elements. MARK URBAN, *THE MAN WHO BROKE NAPOLEON’S CODES* 127–28 (2001). Its deciphering by the British is alleged to have contributed to his defeat. *See id.* at 191–93 (noting the value of the information that deciphering the code gave to the British).

16. DAVID KAHN, *THE CODEBREAKERS: THE COMPREHENSIVE HISTORY OF SECRET COMMUNICATION FROM ANCIENT TIMES TO THE INTERNET* 421–23 (1996).

17. The Soviet Union used two layers of encipherment with telegrams: the Soviets would translate a plaintext message into code using a code book and then encrypt the message with random numbers taken from a set of “one-time pads,” the pads being “theoretically indecipherable as long as the pads were used only once.” Ellen Schrecker, *Stealing Secrets: Communism and Soviet Espionage in the 1940s*, 82 N.C. L. REV. 1841, 1846 (2004); *see also* JOHN EARL HAYNES & HARVEY KLEHR, *VENONA: DECODING SOVIET ESPIONAGE IN AMERICA* 25–28 (1999) (detailing the Soviet two-step enciphering process).

18. Palfreyman, *supra* note 2, at 350.

technology, encryption software programs¹⁹ can render data virtually indecipherable without access to the appropriate encryption key²⁰ or password.²¹

As Professor Orin S. Kerr has explained, because “encryption keys are in most cases impossible to guess—trying to guess a single key could occupy a supercomputer for millions of years—encryption offers Internet users” and users of computer encryption generally a degree of privacy in electronic “communications that remains unequaled in the physical world.”²² Unbreakable computer encryption has the potential to give spies, terrorists, hackers, child pornographers, and members of organized crime a powerful weapon to shield their communications from the U.S. government.²³

II. The Historical Problem of Introducing Decrypted Information as Evidence in National Security Prosecutions Without Exposing Sources and Methods

The U.S. government has wrestled with the issue of using deciphered information in national security cases without endangering sources and methods for decades. An example of the difficulty of using and authenticating national security information in prosecutions can be seen in the decision of the FBI not to use information from the Venona decryption program in espionage prosecutions. In February 1943, the U.S. Army’s Signal Intelligence Service, “the precursor to the National Security Agency, began a secret program . . . later codenamed VENONA,” whose initial mission “was to examine and exploit Soviet diplomatic communications[,] but after the program began, the message traffic included espionage efforts as well.”²⁴ The intercepted cables had been sent “between Moscow and the United States (mainly to and from contacts in New York and Washington).”²⁵ The cables

19. Some of these encryption programs, such as Pretty Good Privacy (PGP), are publicly available. See Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a “Reasonable Expectation of Privacy?”*, 33 CONN. L. REV. 503, 503 n.2 (2001) (explaining that PGP is a free software program that “uses public-key encryption to protect e-mail and data files”); PGP CORP., CORPORATE BACKGROUNDER 4 (2008), <http://download.pgp.com/pdfs/datasheets/PGP-Corporate-Backgrounder.pdf> (describing the background and history of PGP Corporation).

20. See Palfreyman, *supra* note 2, at 350 (explaining that an encryption key is “essentially a very long string of numbers whose length makes it extremely hard to memorize”).

21. See *id.* (explaining that a password activates an encryption key and is shorter and more easily remembered).

22. Kerr, *supra* note 19, at 503.

23. See *The Encryption Debate: Criminals, Terrorists, and the Security Needs of Business and Industry: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the S. Comm. on the Judiciary*, 105th Cong. 5 (1997) (statement of Sen. Patrick Leahy, Member, S. Comm. on the Judiciary) (acknowledging awareness of “‘bad’ uses of encryption by criminals” and spies).

24. National Security Agency, Venona (Jan. 15, 2009), http://www.nsa.gov/public_info/declass/venona/index.shtml. The first of six public releases of decrypted Venona messages was not made until 1995. *Id.* This release was followed by five more releases that made public all of the approximately 3,000 Venona translations. *Id.*

25. DANIEL PATRICK MOYNIHAN, *SECRECY: THE AMERICAN EXPERIENCE* 61 (1998).

were both coded and enciphered,²⁶ and “it remains a marvel” that approximately 2,900, a fraction of the thousands intercepted, “were ever broken.”²⁷

The information gained through this program “provided U.S. leadership with insight into Soviet intentions and treasonous activities of government employees” until the program ended in 1980.²⁸ The Venona decrypts showed the accuracy “of the information about Soviet espionage” that defecting Soviet agents “Whittaker Chambers (beginning in 1939) and Elizabeth Bentley (beginning in 1945) had provided to the American government.”²⁹ Ultimately, the Venona decrypts provided “some two hundred names or code names of Americans who were passing secret information to Soviet agents.”³⁰ The Venona files “are most famous for exposing Julius and Ethel Rosenberg . . . [and] the Soviets’ efforts to gain information on the U.S. Atomic bomb research and the Manhattan Project.”³¹ Additionally, the Commission on Protecting and Reducing Government Secrecy, chaired by Senator Daniel Patrick Moynihan, found that the Venona files settled the question of the complicity of Alger Hiss and Harry Dexter White.³²

This decrypted information created a dilemma for the U.S. government. The government had devastating evidence regarding Soviet spies that would facilitate—and in some cases make possible—their prosecution. However,

26. *See supra* note 17.

27. MOYNIHAN, *supra* note 25, at 61. Although the team began breaking some of the cables in the summer of 1946,

[t]he arduous decoding work began in 1943 and was done at Arlington Hall, a former girls’ school in Virginia; the setup resembled that of the Ultra project at Bletchley Park in wartime Britain, where German signals were intercepted and decoded. But unlike the British team, which had a smuggled copy of the encoding machine used by the Germans, the American team had only the coded cables themselves. Led by Meredith Knox Gardner, the code-breakers put in much hard work during World War II, but they broke nothing.

Id.; *see also* CHRISTOPHER ANDREW, FOR THE PRESIDENT’S EYES ONLY: SECRET INTELLIGENCE AND THE AMERICAN PRESIDENCY FROM WASHINGTON TO BUSH 178 (1995) (explaining how the volume of intelligence telegraphed to Moscow from the United States in the last year of World War II led to the reuse of one-time pads and made the cipher system vulnerable).

28. National Security Agency, *supra* note 24.

29. MOYNIHAN, *supra* note 25, at 61; *see also* HAYNES & KLEHR, *supra* note 17, at 93–115, 122–23, 150–51 (describing Elizabeth Bentley’s espionage activities for the Soviet Union and her defection); *id.* at 65–67, 125–26, 137–39, 227–28 (describing Whittaker Chambers’s espionage activities and his defection). For more in-depth, comprehensive treatments of Bentley and Chambers, *see generally* KATHRYN S. OLMSTED, RED SPY QUEEN: A BIOGRAPHY OF ELIZABETH BENTLEY (2002) and SAM TANENHAUS, WHITTAKER CHAMBERS (1997).

30. MOYNIHAN, *supra* note 25, at 62.

31. National Security Agency, *supra* note 24.

32. COMM’N ON PROTECTING AND REDUCING GOV’T SECRECY, REPORT OF THE COMMISSION ON PROTECTING AND REDUCING GOVERNMENT SECRECY, S. DOC. NO. 105-2 app. A, at A37 (1997) (“The complicity of Alger Hiss of the State Department seems settled. As does that of Harry Dexter White of the Treasury Department.”); *see also* MOYNIHAN, *supra* note 25, at 146 (explaining that “[w]ith the publication of the Venona documents, the evidence of Hiss’s guilt became public” and that “Hiss was indeed a Soviet agent and appears to have been regarded by Moscow as its most important”).

using the evidence in such prosecutions would risk exposing the sources and methods the government used to obtain the evidence.³³ In a 1956 memo, Assistant Director of the Domestic Intelligence Division of the FBI Alan H. Belmont counseled against introducing Venona information into evidence in the espionage prosecution of Judith Coplon—an analyst who had worked in the Foreign Agents Registration section of the U.S. Department of Justice, had access to FBI counterespionage files, and was arrested by the FBI in 1949 while handing over some of those files to a KGB officer.³⁴ He also advised against using Venona information in prosecutions of the Perlo group—which developed Soviet sources on the War Production Board, on a key Senate committee, and in the Treasury Department³⁵—and the Silvermaster group—which established contacts “not only in [the] Treasury and the Army Air Force but in the White House itself.”³⁶ Despite recognizing that the introduction of this evidence “could be the turning point” in such cases, and acknowledging that such information had been used in investigations that resulted in cases against a number of individuals, he concluded that attempting to use this information for prosecution “would not be in the best interests of the U.S. or the Bureau.”³⁷ Ultimately, the government was unsuccessful in its two attempts to prosecute Coplon³⁸ and did not prosecute the members of the Silvermaster³⁹ and Perlo groups.⁴⁰

A significant factor in the FBI’s decision was the potential disclosure of sources and methods that would have arisen from introducing the

33. Protecting sources and methods remains an issue. See 50 U.S.C. § 403-1(j)(1) (2006) (“The Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure.”). The Key Theory described below presumes that the U.S. government is willing to disclose the fact that it can acquire and decrypt the information.

34. Memorandum from A.H. Belmont to L.V. Boardman (Feb. 1, 1956), in VENONA: FBI DOCUMENTS OF HISTORIC INTEREST 70–72, available at <http://foia.fbi.gov/venona/venona.pdf>; see also HAYNES & KLEHR, *supra* note 17, at 3, 158–60 (describing the intercepted communications concerning Coplon, her arrest, and the problems associated with the use of the communications in her prosecution).

35. See HAYNES & KLEHR, *supra* note 17, at 116–29 (describing the Perlo group’s members and their espionage activities).

36. *Id.* at 116.

37. Memorandum from A.H. Belmont to L.V. Boardman, *supra* note 34, at 61–62. Belmont described how such information had been used in investigations that led to the prosecution of, *inter alia*, Judith Coplon and Julius and Ethel Rosenberg, and how those “prosecutions were instituted without using [the] information in court.” *Id.* at 62. Additionally, the memorandum includes a handwritten note at the end of the summary of Belmont’s analysis that appears to be from FBI Director J. Edgar Hoover stating, “I agree.” *Id.*

38. See HAYNES & KLEHR, *supra* note 17, at 159–60 (describing how Coplon was tried and convicted twice, but each time an appellate court ordered a new trial after finding key evidence inadmissible due to lack of probable cause and attributing these findings to the government’s decision not to produce Venona decryptions and show that the decryptions were the basis of its actions).

39. See JOHN EARL HAYNES & HARVEY KLEHR, EARLY COLD WAR SPIES 32 (2006) (discussing the Silvermaster group and noting that “none of those . . . accused were ever convicted, or even indicted, for espionage”).

40. HAYNES & KLEHR, *supra* note 17, at 129.

information as evidence.⁴¹ Specifically, the FBI was concerned that defendants would request that privately hired cryptographers be allowed to examine the encrypted messages and the work of the government's cryptographers to exonerate their clients.⁴² Disclosure of this information and work, the FBI feared, would lead to the exposure of U.S. government techniques and practices in the field of cryptography to unauthorized persons and thus compromise the government's efforts in the communications intelligence field.⁴³ Also, this course could lead to the exposure of pending investigations.⁴⁴

III. The Requirement of Authentication

The Federal Rules of Evidence provide federal courts with wide latitude in authenticating evidence. Federal Rule of Evidence 901 sets forth the following general test: "The requirement of authentication . . . as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."⁴⁵ In other words, as long as there is sufficient evidence for a reasonable juror to find that the item is "genuine (or in the case of illustrative evidence, that it fairly and accurately depicts what it is claimed to illustrate), the authentication threshold is met."⁴⁶ The trial court does not need to determine that an item is

41. See Memorandum from A.H. Belmont to L.V. Boardman, *supra* note 34, at 70 (referencing the potential exposure of techniques and practices).

42. See *id.* (expressing concern that because the government would need its cryptographers to testify as experts for the information, the defense would request and would be permitted to have its own cryptographers examine not only information the government sought to introduce as evidence but all messages that were not decrypted).

43. *Id.*

44. Additionally, the FBI was concerned with, *inter alia*, the damage to the United States' efforts in the counterespionage field "if the Soviets learn[ed] of the degree of success" the United States had achieved in breaking the Soviets' codes—a consideration, as discussed above, that the government has to decide is outweighed by the need for prosecution before applying the Key Theory. *Id.* at 62. Unbeknownst to the U.S. government, the Soviets already knew that the United States had partially broken their codes "thanks to a spy among the code-breakers and thanks also to Soviet spy Kim Philby, British intelligence's liaison to the American intelligence services, whom the proud code-breakers had invited to tour Arlington Hall." MOYNIHAN, *supra* note 25, at 16. Some other concerns of Belmont's were as follows:

the question of law involved—whether or not the [redacted] information would be admitted into evidence as an exception to the hearsay evidence rule; . . . the fragmentary nature of the messages and the extensive use of cover names therein make positive identifications of the subjects difficult; . . . the political implications in this an election year; . . . the international repercussions and resultant Soviet propaganda when it is disclosed that the U.S. intercepted and worked on breaking Soviet coded messages when the countries were allied against the Axis"

Memorandum from A.H. Belmont to L.V. Boardman, *supra* note 34, at 61–62.

45. FED. R. EVID. 901(a).

46. Steven Goode, *The Admissibility of Electronic Evidence*, 29 REV. LITIG. 1, 8 (2009).

authentic; rather it only needs to “determine that a reasonable juror could find that the item is authentic.”⁴⁷

Rule 901(b) provides nine examples of how materials can be authenticated.⁴⁸ The Rule specifically states that these examples are “[b]y way of illustration only, and not by way of limitation,”⁴⁹ and the Advisory Committee’s note expands on this idea stating that the examples are “meant to guide and suggest, leaving room for growth and development in this area of the law.”⁵⁰ Of these examples, the three most relevant to the instant analysis of the Key Theory are Rule 901(b)(1) (“Testimony of witness with knowledge. Testimony that a matter is what it is claimed to be.”),⁵¹ Rule 901(b)(4) (“Distinctive characteristics and the like. Appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances”),⁵² and Rule 901(b)(9) (“Process or system. Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.”).

Additionally, the first two of these examples can be combined in the chain-of-custody doctrine to create “a hybrid form” of Rule 901(b)’s “listed methods.”⁵³ The chain-of-custody doctrine “involves both the testimony of one or more witnesses with knowledge [Rule 901(b)(1)] . . . and the distinctive characteristics of the evidence, taken in conjunction with circumstances [Rule 901(b)(4)].”⁵⁴ This doctrine applies to evidence that “is not readily identifiable and is susceptible to alteration by tampering, decay, or contamination.”⁵⁵ The litigant seeking to introduce such evidence must authenticate it by demonstrating “what the evidence was when gathered and that it has remained unchanged since then.”⁵⁶ The litigant must account for

47. *Id.*; see also *United States v. Gagliardi*, 506 F.3d 140, 151 (2d Cir. 2007) (recognizing the standard for authentication as “minimal”).

48. FED. R. EVID. 901(b)(1)–(9). Rule 901(b)(10) incorporates any other methods recognized by statute or court rule.

49. *Id.* R. 901(b).

50. *Id.* R. 901 advisory committee’s note.

51. Rule 901(b)(1) “contemplates a broad spectrum” of testimony, including testimony of a witness “accounting for custody through the period until trial, including laboratory analysis.” *Id.*

52. The Advisory Committee’s note on Rule 901 explains:

[C]haracteristics of the offered item itself, considered in the light of circumstances, afford authentication techniques in great variety. Thus a document . . . may be shown to have emanated from a particular person by virtue of its disclosing knowledge of facts known peculiarly to him . . . ; similarly, a letter may be authenticated by content and circumstances indicating it was in reply to a duly authenticated one.

Id.

53. 5 JACK B. WEINSTEIN & MARGARET A. BERGER, WEINSTEIN’S FEDERAL EVIDENCE § 901.03[3] (Joseph M. McLaughlin ed., 2d ed. 2008).

54. *Id.*

55. *Id.*

56. *Id.*

the item from the time of seizure by law enforcement until presentation at trial.⁵⁷

Further, Federal Rule of Evidence 803(6)—under which records of regularly conducted activity are not excluded by the hearsay rule—can be used to bring into evidence information that is a record of regularly conducted business activity.⁵⁸ The element of unusual reliability of business records is said variously to be supplied by “systematic checking, by regularity and continuity which produce habits of precision, by actual experience of business in relying upon them, or by a duty to make an accurate record as part of a continuing job or occupation.”⁵⁹

The next Part discusses how the Key Theory works, both in theory and practice, and how the Rule 901(b) examples, the chain-of-custody doctrine, and the hearsay exception for records of regularly conducted activity can be used to authenticate plaintext derived from ciphertext under the Key Theory.

IV. The Key Theory: The Concept and How It Can Be Applied

Under the Key Theory, the government can authenticate decrypted information and have it admitted into evidence in court if it can demonstrate an unbroken chain of custody of the encrypted information or that the encrypted information is a record of a regularly conducted activity, and that a decryption key, password, or other means of decryption in its possession can decrypt the encrypted information. The government does not need to explain how the key, password, or other means of decryption was obtained or created.

The reasoning behind the Key Theory is that an encryption key or password, like a key to a locked door, simply makes accessible something already in existence; it does not alter the encrypted information or create something new. Decryption is a binary process: the key or password either deciphers or does not decipher the information. Further, just as it would not be necessary or efficient for a police officer to testify to issues regarding metallurgy or locksmithing as part of testifying that a key opens a locked door, a government witness demonstrating the Key Theory should not have to explain how the decryption process works. Therefore, for the purposes of authentication in litigation establishing admissibility, it should be sufficient to show that the encrypted information has remained unchanged since the government seized it or that it was a record of a regularly conducted activity and that the key or password deciphers the information.

57. *Id.*

58. FED. R. EVID. 803(6).

59. *Id.* R. 803(6) advisory committee’s note.

A. *The Method of Applying the Key Theory*

The method of applying the Key Theory is flexible and can be adapted to different circumstances. The basic elements of the Key Theory process are based on Federal Rules of Evidence 901 and 803(6)⁶⁰ and are: (1) showing either (a) that the government has maintained an unbroken chain of custody of the encrypted information, or (b) that the encrypted information is a record of a regularly conducted activity; and (2) providing a demonstration to the district court and jury of how the key or password decrypts a particular kind of encryption.

As an initial matter, to promote efficiency and relevance, the government should, in most cases where the Key Theory is applied, seek factual narrative testimony rather than expert testimony from its witnesses. That is, the prosecution can have a witness, who may or may not have expertise in the area as an incidental matter, testify in a factual manner—for instance, describing the process or steps he followed to decrypt the information—without the witness offering any opinions or even a non-opinion description of scientific processes. Having a witness present factual narrative testimony promotes a relevant and focused factual inquiry and efficient use of the time of the judge, jury, and litigants, which is encouraged by the Federal Rules of Evidence.⁶¹ The Key Theory is a simple process—a witness demonstrates that a key or password decrypts encrypted information—and does not require a witness to provide an opinion based on scientific, technical, or other specialized knowledge. Further, having a witness provide factual narrative testimony promotes trial efficiency. The government can use a single witness to show how encrypted information was seized and either that an unbroken chain of custody has been maintained or that the encrypted information was part of regular business records and then demonstrate the Key Theory. This provides a more streamlined process than having one witness testify to the former and a second testify to the latter. Calling a witness who only provides factual narrative testimony also promotes a more focused inquiry on cross-examination because such a witness, not held out as an expert, is not subject to the same kind of distracting and elaborate questioning about background and experience.⁶² Thus, employing witnesses to present the Key Theory who limit their testimony to factual narrative testimony helps pare back the case to its basic and essential elements and prevents detours into irrelevant and time-consuming areas of inquiry.⁶³

60. *See supra* Part III.

61. *See, e.g.*, FED. R. EVID. 403 (excluding relevant evidence if its admission would be inefficient).

62. *See id.* R. 702 (requiring a witness who testifies as an expert to be “qualified as an expert by knowledge, skill, experience, training, or education”).

63. Choice of witnesses and limits on their examination can also be affected by motions in limine before the trial. *See id.* R. 103 (governing the procedure for admitting and excluding

1. *Chain of Custody.*—Demonstrating that the government has maintained an unbroken chain of custody generally lays a foundation for the introduction of the decrypted information into evidence. It also specifically sets the stage for the government’s demonstration that the encryption key or password decrypts the information by showing that the government has in no way altered the information. It defuses any argument by opposing counsel that the key or password that the government presents in its demonstration is not a real key to the seized encrypted material but is instead a key to a version of the encrypted material altered by the government to implicate their client.

As mentioned above, the chain-of-custody doctrine is a hybrid of Federal Rule of Evidence 901(b)(1) (“Testimony of witness with knowledge. Testimony that a matter is what it is claimed to be.”) and Rule 901(b)(4) (“Distinctive characteristics and the like. Appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances.”).⁶⁴ Prosecutors can use these two rules in the context of the Key Theory to have a government fact witness explain how the materials were seized, preserved, and not altered—in other words, that the encrypted materials being presented in court are the same as the encrypted materials originally seized—and to show how the materials are tied to the defendant.

Specifically, the government, when applying the Key Theory, could have a fact witness testify that the encrypted materials were obtained through a lawful search and seizure pursuant to a warrant. The witness can tie the encrypted materials to the defendant by explaining, for example, how the materials were seized from the defendant’s residence or work place. The witness can then explain how he or she entered either the original version or an original unaltered copy—in the instance of a surreptitious search where it was necessary to make a copy rather than taking the original so that the defendants would not contemporaneously know the search occurred—of the encrypted information into evidence. In some instances, it may be possible for the witness to testify that he or she ensured the integrity of the original through a means such as write protecting a disk. The witness can then testify that he or she made true and accurate copies of this information to use as work copies. The government can use the work copies to examine and possibly decipher the encryption. The original or original unaltered copy will be entered into evidence. Upon the defendant’s request, under the Federal Rules of Criminal Procedure, the government may be required to provide access to

evidence); GLEN WEISSENBERGER, *WEISSENBERGER’S FEDERAL EVIDENCE* § 1.03.4 (6th ed. 2009) (“[M]otions [in limine] may be made by either the party seeking admission or the party seeking exclusion, and are usually (although not always) made before trial.”).

64. See *supra* notes 53–57 and accompanying text.

the original seized encrypted materials to the defense to inspect and copy; it also may choose to provide the defense a copy.⁶⁵

2. *Records of Regularly Conducted Activity*.—For certain types of evidence, such as acquisition of high-frequency radio transmissions, because the evidence was gathered as part of a regularly conducted activity, the record may be admissible pursuant to Federal Rule of Evidence 803(6).

3. *Demonstration*.—After the government has used the chain-of-custody doctrine to show that the encrypted materials have not been altered, the government can then demonstrate, pursuant to Federal Rule of Evidence 901(b)(9) (“Process or system. Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.”), that the ciphertext corresponds to the proffered plaintext because the process of applying the key or password to the ciphertext results in the decryption of the information. The Advisory Committee’s note explains that Rule 901(b)(9) is “designed for situations in which the accuracy of a result is dependent upon a process or system which produces it,” and cites the examples of x-rays and computers.⁶⁶ The note also states that Example 9 “does not, of course, foreclose taking judicial notice of the accuracy of the process or system.”⁶⁷ This example can be used in the context of the Key Theory to show that in the process of decryption, when the key or password the government offers is used, it decrypts the encrypted information. The accuracy of the process or system can be seen in the fact that the key or password produces coherent plaintext rather than incoherent ciphertext.

The government should not have to demonstrate in court the decryption of all the files that are unlocked by the key and password to enter the files into evidence. It should be sufficient to have a government witness illustrate or describe the decryption on one document and then have the witness testify that the key or password similarly decrypted the other encrypted information the government seeks to introduce into evidence. The information can then be entered into evidence.

4. *Two Approaches to Applying the Key Theory*.—Depending on the circumstances of a case, the government may choose to take one of two approaches to implementing the Key Theory. First, the government, particularly in instances where there is a strong need to protect sensitive

65. See FED. R. CRIM. P. 16(a)(1)(E) (providing that “[u]pon a defendant’s request, the government must permit the defendant to inspect and to copy” tangible objects obtained from the defendant or that the government intends to offer in evidence).

66. FED. R. EVID. 901 advisory committee’s note.

67. *Id.* To the extent that a district court has questions about sources and methods and the way the decryption was accomplished, one way to address the court’s concerns might be through the use of procedures in the Classified Information Procedures Act, 18 U.S.C. app. 3 (2006).

sources and methods, can take a guarded approach. In this approach, the government only shows that the key or password decrypts the encrypted information and does not provide testimony regarding where or how the key or password was found or how it works. Second, the government may employ a rich-context method. Under this approach, in addition to showing that the key or password decrypts the encrypted information, the government can provide general information on where it found the key or password, explain generally how the key or password works, or both. The government would not have to explain: (1) how it knew where to find the key or password, (2) how it learned how the key or password works, or (3) the mechanics behind the key or password's operation.

B. The Key Theory in Practice: The Wasp Network Case

The *Wasp Network Case* provides helpful examples of how the government can apply a rich-context version of the Key Theory in litigation. However, although instructive, these examples should not obscure that a more austere, guarded Key Theory approach is also available.

1. *Background.*—On June 8, 2001, a federal jury in the U.S. District Court for the Southern District of Florida convicted five agents of the Directorate of Intelligence, Cuba's primary intelligence agency, of covert activity in the United States (including, as to three defendants, conspiracy to commit espionage)⁶⁸ concluding a multi-month trial that showed “a committed band of spies working to infiltrate South Florida's military installations and Cuban exile community.”⁶⁹ All five defendants were convicted of acting within the United States as agents of a foreign government without notification to the Attorney General, and also of conspiracy to do so and to defraud the United States concerning its governmental functions.⁷⁰ Three members of the group were convicted of conspiracy to commit espionage related to their efforts to penetrate military bases.⁷¹ One member of the group, Gerardo Hernandez, was found guilty of conspiracy to commit murder in connection with the deaths of four fliers from the “Brothers to the Rescue” Cuban-exile

68. See *United States v. Campa*, 529 F.3d 980, 991 (11th Cir. 2008) (detailing the convictions of Gerardo Hernandez, Rene Gonzalez, Antonio Guerrero, Ruben Campa, and Luis Medina), *cert. denied*, 129 S. Ct. 2790 (2009). The U.S. Court of Appeals for the Eleventh Circuit affirmed all convictions. *Id.* at 1018. While affirming all convictions, the Eleventh Circuit remanded the cases of three of the defendants for resentencing. *Id.* Resentencing occurred in October and December 2009; two of those defendants appealed, and the appeals are pending. Notice of Appeal, *United States v. Hernandez*, No. 98-0721-CR-JAL (S.D. Fla. Dec. 22, 2009).

69. Sue Anne Pressley, *Five Cuban Agents Guilty of Spying on U.S.*, WASH. POST, June 9, 2001, at A12.

70. Associated Press, *5 Cubans Convicted in Plot to Spy on U.S.*, N.Y. TIMES, June 9, 2001, at A12.

71. *Id.* Five other indicted members of the group pleaded guilty; some received reduced sentences in light of substantial assistance to the government. *Id.* Four indicted defendants were not arrested and are believed to be in Cuba. *Id.*

group—a “Miami-based organization that flew small aircraft over the Florida Straits in efforts to aid rafters fleeing Cuba”⁷²—who were shot down in 1996 in international airspace by Cuban MiGs.⁷³ The prosecution showed that Hernandez was instructed to steer fellow spies who had infiltrated Brothers to the Rescue away from targeted flights⁷⁴ and was instructed to deliver a message to Havana that led up to the shoot down.⁷⁵

In 1998, the agents were indicted as part of the 14-member, Florida-based spy group, who were known within the Directorate of Intelligence as *La Red Avispa*, or the Wasp Network.⁷⁶ The prosecution established that the defendants were referenced in their communications by code names, and that several were present in the United States under false identities, with false documentation and false life stories,⁷⁷ as the group followed through on assignments to penetrate Cuban-exile political groups and U.S. military installations—including Southern Command, which supervises U.S. military activities in the Caribbean and Latin America.⁷⁸

Prosecutors presented a case based largely on more than 1,200 pages of decrypted communications seized before or at the time of the defendants’ arrests in 1998.⁷⁹ A juror interviewed after the verdict said that the covert documents were the prosecution’s best evidence.⁸⁰ “It wasn’t the complete case, but it was damaging,” the juror said.⁸¹ “There wasn’t much the defense could say about them. They were found in their apartments, and they said a lot of damaging things.”⁸²

2. *Application of the Key Theory in the Wasp Network Case.*—In the *Wasp Network Case*, the prosecution could be characterized as having used what is described above as a rich-context version of the Key Theory method to authenticate decrypted information related to the Wasp Network and its activities. A close examination of how the prosecution authenticated

72. *Campa*, 529 F.3d at 988.

73. Pressley, *supra* note 69.

74. *Campa*, 529 F.3d at 988.

75. Pressley, *supra* note 69.

76. *Id.*

77. The difference between code names and false identities is that all defendants were referred to among themselves by code names, such as “Giro” and “Iselin,” but only some of the defendants, the careerist illegal intelligence officers, operated under false identities. See Brief for the United States at 10 n.9, *United States v. Campa*, 419 F.3d 1219 (11th Cir. 2005) (Nos. 01-17176, 03-11087) (“As part of the compartmentalization and secrecy that are hallmarks of intelligence networks . . . , defendants all had code names apart from false identities.”); *id.* at 4 (“[I]llegal intelligence officers . . . enter the U.S. illegally under false identities such as Hernandez, Medina and Campa . . .”).

78. Pressley, *supra* note 69.

79. Associated Press, *supra* note 70.

80. Gail Epstein Nieves, *Juror: Disk Made Spy Case Easy*, MIAMI HERALD, June 12, 2001, available at 2001 WLNR 3885684.

81. *Id.*

82. *Id.*

decrypted information from computer diskettes and high-frequency radio transmissions shows how the Key Theory can be applied in practice. The following subsections explain how the prosecution authenticated information that was decrypted using three decryption programs: Micro Star, The Typist, and Find.

a. Micro Star Decryption Program.—The prosecution first used what could be seen as a version of the Key Theory method during the direct examination of FBI Special Agent Vicente M. Rosado to introduce into evidence information on computer diskettes decrypted using the Micro Star program. Mr. Rosado was an FBI Special Agent assigned to the Computer Analysis Response Team—a group based in the FBI headquarters laboratory whose function is to “process and analyze computer evidence”—and he had a duty responsibility for “[f]oreign counter intelligence” related to Cuba.⁸³ He laid a foundation for the introduction of the evidence related to Micro Star by showing that he had participated in lawful searches and seizures (including surreptitious searches and seizures) based on warrants⁸⁴ and that the evidence had been held in an unbroken chain of custody and had not been altered.⁸⁵ He then demonstrated to the judge and jury how a password applied to a decryption method decrypted the information.⁸⁶

i. Chain of Custody.—In laying the foundation for admitting the evidence during direct examination by a federal prosecutor, Mr. Rosado first explained how the Government copied 981 disks during lawful searches of the residences of members of the Wasp Network.⁸⁷ Mr. Rosado explained that during the investigation of the Wasp Network his job was to use a machine to “copy computer evidence as found in the residence[s]” and “make sure no trace was left that [he] had been present [He] would just make [his] copies on site and leave everything as it was.”⁸⁸ Mr. Rosado also explained that the entries he made were pursuant to federal court orders for each time period at issue.⁸⁹ These searches and seizures culminated in a final overt search and seizure, pursuant to a search warrant, at the time that the defendants were arrested.⁹⁰

In addition to explaining the search and seizure process, Mr. Rosado explained the process he used to preserve the integrity of the diskettes he had

83. Transcript of Record at 1730, *United States v. Hernandez*, No. 98-0721-CR-JAL (S.D. Fla. 2001).

84. *Id.* at 1734–36.

85. *See id.* at 1745–48 (detailing for the court how he copied the disks, ensured they could not be overwritten, and placed them into evidence).

86. *Id.* at 1772–80.

87. *Id.* at 1898–99, 1902–03.

88. *Id.* at 1744.

89. *Id.* at 1736, 1748–52, 1754.

90. *Id.* at 1807.

made. To protect the diskettes he was downloading data onto and to prevent them from being altered or changed after he had copied data onto them, Mr. Rosado “moved a tab on the computer disk which write protects the diskette so no one else could write to it.”⁹¹ He then made copies of the diskettes he had made and “took the originals and placed them into our evidence.”⁹² These copies were “work copies” and were “true and accurate reproductions of the files that appeared on the disks” he had copied while searching the residences.⁹³

ii. Demonstration.—After laying this evidentiary foundation that, among other things, showed that the encrypted information had not been altered in any way, Mr. Rosado explained and demonstrated how a password used in conjunction with a decryption method decrypted information on the disks. At first, a large majority of the disks appeared to be “empty” or “appeared to have regular files.”⁹⁴ Mr. Rosado used a laptop computer to show what a computer diskette is, how it is read using a computer, and what a blank disk looks like.⁹⁵ He then inserted a copy of a diskette, which was entered into evidence as Exhibit D2, obtained during a search of the apartment of a member of the Wasp Network and showed that although it appeared blank when he checked the diskette’s directory and did a check-disk inquiry, he was eventually “able to find data on that disk.”⁹⁶ Mr. Rosado found that some of the program files⁹⁷ found on other disks “acted on the apparent blank disk in order to decrypt or bring forth data.”⁹⁸ These files did not declare themselves to be decryption or “breakout” programs and were not labeled as such; rather they appeared to be everyday commercial programs.⁹⁹

The prosecutor then asked Mr. Rosado to place another copy of a disk made during a search of a defendant’s apartment, labeled Exhibit D3 and subsequently entered into evidence, into his laptop.¹⁰⁰ Mr. Rosado opened what appeared to be a word processing program on the disk called Micro Star, and he confirmed that there were no files on the disk other than a file explaining how to use Micro Star.¹⁰¹ He then testified that if one used the word processor’s open command on such a disk, ordinarily one would not

91. *Id.* at 1747.

92. *Id.* at 1748.

93. *Id.*

94. *Id.* at 1764.

95. *Id.* at 1759, 1763.

96. *Id.* at 1765–66.

97. A program file is “[a]n electronic file containing commands and instructions for execution by a computer.” WEBSTER’S NEW WORLD TELECOM DICTIONARY 392 (2008).

98. Transcript of Record, *supra* note 83, at 1767.

99. *Id.*

100. *Id.* at 1768.

101. *Id.* at 1770–71.

expect entering a name would access a file.¹⁰² He then showed that when he went to the “open” command and typed the password *afinacion* or entered that file name, the program asked him to “insert a diskette.”¹⁰³ Mr. Rosado testified that ordinarily when one tries to open a specific word processing file, one would expect the program would either show the text of the file or say that no text exists.¹⁰⁴ After this explanation, Mr. Rosado inserted Exhibit D2, the diskette that had previously seemed to be blank, and three different documents in Spanish, which would print out to several pages of text, appeared on the computer screen.¹⁰⁵ Mr. Rosado testified that he had previously reviewed the Spanish-language text, and it was a report that referenced, among other things, Brothers to the Rescue activities; it was from “Iselin,” a code name for defendant Rene Gonzalez, to “Giro,” a code name for defendant Gerardo Hernandez;¹⁰⁶ and it appeared to be an account of meetings and results of meetings.¹⁰⁷ He explained that the text included two additional reports.¹⁰⁸

The prosecutor then further examined Mr. Rosado, laying a foundation for these files and numerous other decrypted files to be entered into evidence. The prosecutor presented three notebooks containing government files depicting Mr. Rosado’s “work product” in printed-out form.¹⁰⁹ Mr. Rosado explained that when he went through this disk and others like it, he saved the decrypted information to another disk or printed it out in decrypted form.¹¹⁰ He testified that those pages “truly and accurately reproduce[d] the files” as he “broke them out from other disks” and that he worked with, broke out, and produced the text for all of the exhibits in the books.¹¹¹ He also testified that he used different decryption files found in programs in addition to the Micro Star program to decrypt some of these disks.¹¹² Following this testimony, the district court admitted into evidence the Government exhibits of the decrypted plaintext Spanish-language files in the three notebooks.¹¹³ Later, English translations were admitted into evidence.¹¹⁴

Mr. Rosado also explained where he obtained the password or key to the Micro Star decryption files and generally how he used the password or

102. *Id.* at 1771–72.

103. *Id.* at 1772.

104. *Id.*

105. *Id.* at 1773.

106. *See* *United States v. Campa*, 529 F.3d 980, 980 (11th Cir. 2008) (stating in the case caption that Rene Gonzalez was also known as Iselin and that Gerardo Hernandez was also known as Giro).

107. Transcript of Record, *supra* note 83, at 1774.

108. *Id.*

109. *Id.* at 1785.

110. *Id.* at 1774–75.

111. *Id.* at 1785–86.

112. *Id.* at 1786.

113. *Id.*

114. *Id.* at 2672.

key with the decryption files. He stated that the word *afinacion* is “a password or key to allow” the Micro Star word processing program “to operate in a manner other than its intended” word processing purpose.¹¹⁵ This password or key is necessary to start the decryption process.¹¹⁶ He also testified and demonstrated to the court on his laptop that this key or password *afinacion* can be found on the same disk as the Micro Star decryption program by using Norton Utilities Disk Editor, a widely available commercial program, to access the sector of the disk that contains the key or password.¹¹⁷ He noted that the word *afinacion* stands out from the other types of characters because it “is a word that doesn’t really fit into what I would expect to find on a disk that has a program.”¹¹⁸

Thus the prosecution can be seen to have used a rich-context version of the Key Theory method with Mr. Rosado to enter into evidence the decrypted information from the specific demonstration file and other files decrypted with the Micro Star decryption program and the password or key *afinacion*. This allowed the prosecution to enter this information into evidence based on data within the parameters of the disks. Although Mr. Rosado provided background on how the government obtained and used the key or password *afinacion* and the Micro Star decryption program, he did not purport to explain or analyze theoretical or scientific concepts of decryption.

b. The Typist Decryption Files.—The prosecution used similar approaches, which could also be seen as applications of the Key Theory, during the direct examinations of Myron Broadwell and Kenneth W. Hart to introduce information from high-frequency radio transmission¹¹⁹ intercepts that had been decrypted with The Typist decryption files found on diskettes from the defendants’ residences. Mr. Broadwell laid the foundation for the admission of records of the encrypted transmissions by explaining how the transmissions were collected and transcribed as a regular professional practice of the FBI, and Mr. Hart demonstrated how The Typist, when used with keys and passwords, decrypted the intercepts.

i. Records of Regularly Conducted Activity.—On direct examination, Mr. Broadwell—a supervisory special agent with the FBI’s investigative-technologies branch of the laboratory division and the supervisor of the Data Collection Facility, whose staff listens to high-frequency broadcasts using shortwave radio receivers¹²⁰—explained the process by which the FBI collected and made a record of the radio transmissions.

115. *Id.* at 1778–79.

116. *Id.* at 1779.

117. *Id.* at 1779–81.

118. *Id.* at 1783–84.

119. *See id.* at 2447 (explaining that high-frequency radio transmissions are “radio transmissions that exist in the frequency bandwidth from approximately 3 to 30 megahertz”).

120. *Id.* at 2444, 2446.

Mr. Broadwell explained that his staff listened to recordings of these radio broadcasts, “transcribe[d] what is generally Morse code being transmitted,” and archived the transcriptions.¹²¹ Mr. Broadwell testified that with the Morse code broadcasts instead “of a voice it would be a series of tones, short and long in the Morse code coding scheme.”¹²² Although these broadcasts are readily audible to anyone who has a commercially available shortwave radio, because the broadcasts are in Morse code, they are not readily comprehensible.¹²³ His staff transcribed the Morse code, which is transmitted in five character groups, into alpha characters—rather than numbers—and typed that into a word processing program for generating a transcript.¹²⁴ He explained that such transcription is a regularly conducted duty or practice of the FBI.¹²⁵

Mr. Broadwell testified that he had been asked to collect or retrieve certain archived transcripts and to place them on storage or transfer media, and then identified a color photocopy of a computer disk that had been received in evidence as one onto which he “copied certain selected transcriptions of high frequency broadcasts”; he also identified a notebook as containing printed-out versions of the retrieved Morse code transcripts.¹²⁶ Additionally, he explained that the transcription appeared as “a series of random letters,” which would not make sense to a person.¹²⁷ The prosecution then moved for admission of the notebook pages reflecting the encrypted text of the messages, and the district court admitted it over the objections of the defense.¹²⁸

The prosecution subsequently moved to admit into evidence similar pages of the notebook reflecting older transcripts through a combination of Federal Rule of Evidence 803(6) and the chain-of-custody doctrine.¹²⁹ Mr. Broadwell testified that during the time the transcriptions were made, such transcriptions were the professionally, regularly conducted activity of the FBI, and that once the transcriptions were made, they were put into “files and placed into safes” and remained within the custody of the data-collection facility.¹³⁰

ii. Demonstration.—With the encrypted information admitted into evidence on this foundation, the prosecution called Mr. Hart to “testify

121. *Id.* at 2447–48.

122. *Id.* at 2448.

123. *Id.*

124. *Id.* at 2449.

125. *Id.* at 2452.

126. *Id.* at 2452–54.

127. *Id.* at 2453.

128. *Id.* at 2457–59.

129. *Id.* at 2488.

130. *Id.*

to the breaking out of these messages into plain text.”¹³¹ Mr. Hart—a computer specialist,¹³² forensic examiner¹³³ for the FBI laboratory division, and member of the Computer Analysis Response Team—testified that he used decryption files that Mr. Rosado had acquired from the defendants’ residences to decrypt the encrypted high-frequency radio messages provided by Mr. Broadwell.¹³⁴

Similarly to Mr. Rosado, Mr. Hart performed a computer demonstration to show how materials seized from the defendants’ residences could be used to decrypt information. Mr. Hart explained that one of the seized disks contained a “program called The Typist, which appeared to be a game” or “tutorial involving typing skills.”¹³⁵

To begin the demonstration, Mr. Hart inserted the disk into the computer—with screens in the courtroom showing the judge, the jury, and the defense the computer screen—and showed the directory of files that appeared on the disk, including The Typist file.¹³⁶ He explained that The Typist file stood out on the disk because it is a boot disk¹³⁷ and “the first four files are DOS operating system files and Typist is on there all alone.”¹³⁸ Mr. Hart then opened The Typist file¹³⁹ and showed how the regular game works.¹⁴⁰

Although The Typist initially appeared to be a regular game, Mr. Hart explained that if he typed the password or key *GIRASOL*, the program stopped acting as a typing-proficiency game and threw up a prompt for a file name.¹⁴¹ This did not appear to be part of the regular game, and the program appeared to have been altered.¹⁴²

Mr. Hart then opened The Typist program, started the game, entered the password *GIRASOL*, and when prompted entered the file name for an encrypted file.¹⁴³ Text then appeared on the screen in the courtroom in Spanish.¹⁴⁴ Mr. Hart explained that he used The Typist program against

131. *Id.* at 2459.

132. *See id.* at 2572 (describing a computer specialist as a “person who extracts, examines and/or produces data from digital related evidence”).

133. *See id.* at 2571 (describing forensic examiners as individuals who “examine and extract and present digital evidence from computers, computer type evidence and storage media”).

134. *Id.* at 2584.

135. *Id.* at 2590–91.

136. *Id.* at 2594.

137. A boot disk is a disk that allows a computer to start. Tech Terms Computer Dictionary, <http://www.techterms.com/definition/bootdisk>. The most common type is an internal hard drive. *Id.*

138. Transcript of Record, *supra* note 83, at 2595.

139. *Id.* at 2595–96.

140. *Id.* at 2596–97.

141. *Id.* at 2599.

142. *Id.*

143. *Id.* at 2605–06.

144. *Id.* at 2606–07.

other texts that appeared in the Government's book of exhibits and was able to obtain plaintext for other messages.¹⁴⁵ He also testified that there were other versions of The Typist program on other disks that were capable of decrypting certain messages that The Typist program he used for his courtroom demonstration could not decrypt.¹⁴⁶ Mr. Hart then testified that the text on the screen was the same as on a page in the Government's exhibit notebook, and the court admitted the page into evidence over the defense's objections.¹⁴⁷

Mr. Hart testified that he applied The Typist program and obtained plaintext for each of the exhibits reflected on a chart that detailed, among other things, the separate exhibits and the means the Government used to decrypt them.¹⁴⁸ Each of the relevant exhibits in the exhibit book had a first page of ciphertext (which was in evidence through Mr. Broadwell's testimony) and a second page of plaintext in Spanish, which Mr. Hart had decrypted using the program disks as enumerated on the chart.¹⁴⁹ The prosecution then moved into evidence approximately thirty-seven decrypted plaintext Spanish exhibits related to The Typist program over the objections of the defense.¹⁵⁰

Mr. Hart also explained the process pointing to the password or key, *GIRASOL*. He testified that the word "was embedded inside the program file itself" and that he found it "mostly by visual inspection."¹⁵¹ He then demonstrated that he could use the program Norton Disk Editor—a utility program that can be used to view low-level data for programs, drives, and files—to view the contents of the executable file The Typist.¹⁵² When he applied Norton Disk Editor, it showed a hexadecimal¹⁵³—a base-16 numbering system—and ASCII—American Standard Code for Information Interchange,

145. See *id.* at 2607 (referencing a chart introduced by the prosecution reflecting that certain messages were capable of being decrypted and producing plaintext using The Typist).

146. *Id.* at 2608.

147. *Id.* at 2610–11.

148. *Id.* at 2616.

149. *Id.*

150. *Id.* at 2616–17. As with the decrypted diskettes, in plaintext Spanish, introduced during Mr. Rosado's testimony, a translator's subsequent testimony later provided the foundation for introduction of the English translations of the decrypted messages introduced through Mr. Hart's testimony, comprising the third page of each tabbed entry in the notebook. See *id.* at 2669 (describing the translated diskette decrypts being entered into evidence); *id.* at 2826 (describing the translated high-frequency radio transmission decrypts being entered into evidence).

151. *Id.* at 2611.

152. *Id.* at 2612.

153. The hexadecimal system is "a different method of representing numbers than the base-10 system [used] in every day practice." Tech Terms Computer Dictionary, <http://www.techterms.com/definition/hexadecimal>. In the hexadecimal system, "each digit can have sixteen values instead of ten." *Id.* For example, "[t]he values of a hexadecimal digit can be: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F." *Id.* Although "computers process numbers using the base-2, or binary system, it is often more efficient to visually represent the numbers in hexadecimal format" because "it only takes one hexadecimal digit to represent four binary digits." *Id.*

the standard character set used by computers and made up of letters, numbers, and symbols—equivalent of the file.¹⁵⁴ He then looked through the ASCII display of the contents of the file, which was quite lengthy, “looking for groups of letters, five to seven characters in length.”¹⁵⁵ In a particular area of the column, he found the letters *HKUEXUS*, which he explained were a cipher for the password or key *GIRASOL*: “Basically you take your first letter and you go backwards one step in the alphabet and you will get the letter G by going back one character” and for the second letter “[y]ou go back two steps in the alphabet and it progresses on through until eventually you wind up with *GIRASOL*.”¹⁵⁶

In this way, the Key Theory can be seen to account for how the prosecution authenticated information derived from The Typist decryption program. The prosecution laid the foundation for entering the information into evidence by having Mr. Broadwell explain how the encrypted information was obtained and Mr. Rosado testify how the decryption programs were seized and preserved. The prosecution built on this foundation by having Mr. Hart testify and demonstrate how the password or key, combined with The Typist program, decrypted the information.

As with Mr. Rosado’s testimony, the prosecution had Mr. Hart explain and demonstrate generally how The Typist program worked and where the password or key was found, but did not present an analytic or theoretical explanation of the decryption or other scientific processes underlying it.

c. Find Decryption Program.—The prosecution also can be seen to have applied the Key Theory in entering information decrypted with the Find decryption program into evidence. Mr. Hart testified that although the last two exhibits in the notebook of exhibits, which were also taken from high-frequency radio transmissions, were not capable of being broken out with The Typist program, another decryption program called Find.EXE on one of the seized disks was able to decrypt the files.¹⁵⁷ He also testified that two of the seized disks contained the decryption key, and another disk had the password, *safelight*.¹⁵⁸ Additionally, Mr. Hart explained that, similar to what he had demonstrated with The Typist program, the password *safelight* was embedded in hexadecimal material.¹⁵⁹

Rather than asking Mr. Hart to perform a computer demonstration of the Find decryption program as he had done with The Typist program, the prosecution had Mr. Hart testify to the process whereby he decrypted the two

154. Transcript of Record, *supra* note 83, at 2612–13.

155. *Id.* at 2613–14.

156. *Id.* at 2614.

157. *Id.* at 2622–23.

158. *Id.* at 2624.

159. *Id.*

files The Typist had been unable to decrypt.¹⁶⁰ He stated that he would start the “Find program much like [he] started the Typist one,” only he “put the password right on the command line of the program. It would be find space then the password used.”¹⁶¹ Instead of getting the find options from using the program, he would then be presented with an options menu screen, in which case he “could receive messages, send messages or exit the program.”¹⁶² At that point, to receive the decryption process, he would use the option to receive the messages; then he would type the name of the file to be decrypted, and the Find program would give the user options for which hard drive to use with the decryption key disk.¹⁶³ Once the user put the decryption key disk in the appropriate hard drive and hit enter, Mr. Hart explained, “if it is the correct disk for that message or program, it will show up on the screen similar to Typist, the translated or decrypted text of your original message.”¹⁶⁴ He then testified that he was able to decrypt the two files described above with this process and that the plaintext in the Government’s exhibit book was the same as the decrypted text he had produced.¹⁶⁵ The district court then admitted the plaintext of these two files in the exhibit book into evidence.¹⁶⁶

Again, the prosecution was able, through what could be characterized as an application of the Key Theory, to move decrypted information into evidence within the parameters of the seized material. The prosecution had the witness generally show what the password was, how the password and decryption keys were discovered, how the decryption program worked, and that it worked on the two files.

Thus, the *Wasp Network Case* provides examples of how the government can carefully authenticate decrypted information according to the principles of the Key Theory by laying a solid evidentiary foundation through the chain-of-custody doctrine or the business-records exception to the hearsay rule and then demonstrating how the key or password decrypts the encrypted information.

V. Defense Arguments Against the Key Theory and Why They Fail

Defense counsel may raise a number of arguments against the Key Theory. The following are the most likely to be raised. For the reasons set forth below, each of these objections is flawed. The common flawed thread in each objection is a lack of acknowledgement of the simple, binary nature of the Key Theory.

160. *Id.*

161. *Id.*

162. *Id.*

163. *Id.* at 2625.

164. *Id.*

165. *Id.* at 2625–26.

166. *Id.* at 2626.

A. Sixth Amendment Confrontation Clause Objection

Under the Sixth Amendment's Confrontation Clause, "[i]n all criminal prosecutions, the accused shall enjoy the right . . . to be confronted with the witnesses against him."¹⁶⁷ In *Crawford v. Washington*,¹⁶⁸ the Supreme Court increased the scope of the Confrontation Clause in trials.¹⁶⁹ Justice Scalia's opinion made any "testimonial" out-of-court statement inadmissible if the accused did not have the opportunity to cross-examine the witness and the witness is unavailable at trial.¹⁷⁰ The Court refused to determine whether laboratory test results are testimonial evidence subject to the Confrontation Clause.¹⁷¹ In *Melendez-Diaz v. Massachusetts*,¹⁷² the Court held that certificates of analysis (which state the results of state laboratory tests) are testimonial evidence that may not be admitted without accompanying live testimony by the analyst who conducted the tests.¹⁷³ Defendants can cross-examine the affiants under their Sixth Amendment right of confrontation.¹⁷⁴

There is little national security case law following these decisions so far. However, it would appear that *Melendez-Diaz* would not apply to the Key Theory process because the government conducts a demonstration in front of the defendant, the judge, and the jury. Further, the witness who performs the demonstration can be cross-examined by the defense. Pursuant to the Federal Rules of Evidence, such cross-examination should be limited to the factual demonstration itself.¹⁷⁵ It should not be necessary to have the demonstrating witness explain scientific concepts related to decryption. A police officer does not have to testify how a key works in a lock or where he found

167. U.S. CONST. amend. VI.

168. 541 U.S. 36 (2004).

169. *See id.* at 60, 68 (condemning the Court's prior Confrontation Clause test as at once overly broad and too narrow, "often fail[ing] to protect against paradigmatic confrontation violations" and devising a new test in which all evidence that could be considered testimonial would be subject to scrutiny under the Sixth Amendment).

170. *Id.* at 68. Testimonial means any statements that an objectively reasonable person in the declarant's situation would have deemed likely to be used in court. *See Davis v. Washington*, 547 U.S. 813, 822 (2006) (holding that statements made in a police interrogation are testimonial when the circumstances objectively indicate that there is not an ongoing emergency and the primary purpose of the interrogation is to discover facts for possible use in a prosecution).

171. *The Supreme Court, 2008 Term—Leading Cases*, 123 HARV. L. REV. 153, 202 (2009); *see also Crawford*, 541 U.S. at 68 ("We leave for another day any effort to spell out a comprehensive definition of 'testimonial.' Whatever else the term covers, it applies at a minimum to prior testimony at a preliminary hearing . . . and to police interrogations.").

172. 129 S. Ct. 2527 (2009).

173. *Id.* at 2542; *see also* Posting of Lyle Denniston to SCOTUSblog, <http://www.scotusblog.com/?s=law+need+not+bow+to+chemistry> (June 25, 2009, 15:36 EST) (summarizing the *Melendez-Diaz* decision).

174. *See Melendez-Diaz*, 129 S. Ct. at 2532 (holding that the defendant was entitled to be confronted with the affiants at trial).

175. *See* FED. R. EVID. 611(b) ("Cross-examination should be limited to the subject matter of the direct examination . . .").

the key to show how he opened a door,¹⁷⁶ and a government witness in an encryption case should not have to testify how a key or password was obtained or works with an encryption program to demonstrate how the key or password decrypts the information.

B. *Brady and Jencks Act Objections*

Defendants could also argue that the Key Theory violates the Supreme Court's *Brady v. Maryland*¹⁷⁷ decision and the Jencks Act.¹⁷⁸ However, because of the binary nature of the Key Theory, *Brady* and Jencks Act obligations should not apply to the demonstration, and the government should follow its *Brady* and Jencks Act obligations regarding the decryption process.

In *Brady*, the Supreme Court ruled that suppression by the prosecution of evidence favorable to a defendant who has requested it violates due process.¹⁷⁹ The prosecutor must disclose evidence or information that would prove the innocence of the defendant or mitigate the defendant's sentence.¹⁸⁰ For example, prosecutors must disclose exculpatory evidence known only to the police.¹⁸¹ The prosecutor has a duty to review the police's investigatory files and disclose anything that tends to prove the innocence of the defendant.¹⁸²

The Jencks Act governs production of statements and reports of prosecution witnesses during federal criminal trials.¹⁸³ The Act provides the following:

In any criminal prosecution brought by the United States, no statement or report in the possession of the United States which was made by a Government witness or prospective Government witness (other than the defendant) shall be the subject of subpoena, discovery, or inspection *until* said witness has testified on direct examination in the trial of the case.¹⁸⁴

Brady and the Jencks Act are not obstacles to the Key Theory. The Key Theory involves a simple mechanical function—a key or password unlocking encrypted information—so *Brady* and the Jencks Act would not apply because the process would not be germane to exculpatory information. The key or password would either work or would not work. If the key or password

176. *See id.* R. 201(b) (describing judicial notice as appropriate when the fact is “generally known within the territorial jurisdiction of the trial court”); *id.* R. 402 (“Evidence which is not relevant is not admissible.”).

177. 373 U.S. 83 (1963).

178. 18 U.S.C. § 3500 (2006).

179. 373 U.S. at 86.

180. *Id.* at 87.

181. *Kyles v. Whitney*, 514 U.S. 419, 438–39 (1995).

182. *Id.*

183. 18 U.S.C. § 3500.

184. *Id.* § 3500(a).

works, there would be no exculpatory information. If the key or password does not work, the materials in question would not be authenticated, and *Brady* and the Jencks Act would not be necessary.

The government should follow its *Brady* and Jencks Act obligations regarding the decryption process.

C. Reciprocity and Multiple Keys

The defense may request to have its experts examine the encrypted information and the password or key. One result of the government allowing the defense to examine the encrypted information is that the defense may produce another key or password that deciphers the ciphertext into different, less incriminating plaintext than that offered by the government. The government can respond to this argument in two ways. First, the government can state that most computer encryption, due to its complexity, will only have one key or password and hide only one plaintext message and that the message that the government has decrypted is the true message. Second, the government can explain that it is possible for an encrypter to combine two encrypted pieces of information into a single file so that a second key will open a second, innocent message and that this disinformation is just another form of encryption. The government can seek to show how this second encryption has been used to hide the incriminating encryption.

The government and the defendant can then ask the trial court, pursuant to Federal Rule of Evidence 104(a) (“Preliminary questions concerning . . . the admissibility of evidence shall be determined by the court . . .”), to authenticate their respective decrypted information and let the fact finder decide which information it should give weight to, considering the totality of the circumstances. To make this request, the defense would have to show that there is a basis for the defense’s version of the decryption. The defense could not just produce a purported plaintext and demand that it be admitted without laying a foundation showing that it was, in fact, decrypted from the ciphertext with an actual key or password. In this way, the government’s sensitive sources and methods would be protected and the relevant information would be authenticated.

D. Defendant Claims Not to Have Been in Possession of Key, Decryption Method, or Encrypted Materials

The defendant may also argue that the plaintext derived from an encrypted file should not be admitted into evidence because either the defendant had the encrypted file but not a key, password, or other decryption method, or the defendant had the decryption method, but the defendant claims it was not in possession of the encrypted information. This objection does not stand because under Federal Rules of Evidence 901 (“Requirement of Authentication or Identification”) and 402 (“Relevant Evidence Generally Admissible; Irrelevant Evidence Inadmissible”), it is only necessary to

produce evidence sufficient to support a finding that the item is what its proponent claims it to be and that it is relevant to the case. Thus, under the Key Theory, it is enough to show that the encrypted information in the possession of the defendant can be opened by a key or password, or that the key or password in possession of the defendant opens the encrypted information and that the encrypted information is relevant to the case in order to authenticate the resulting plaintext and have it admitted into evidence.¹⁸⁵ As long as the trial court authenticates the information and allows it into evidence, the court or jury can decide how much weight to give it.¹⁸⁶

VI. The Key Theory's Applicability to Civil Litigation

Although this Article has focused on the government's ability to use the Key Theory in prosecutions, the legal concepts of the Key Theory are also applicable to admission of evidence in civil cases. Civil litigants could potentially use the Key Theory to protect sources and methods related to national security and trade secrets.¹⁸⁷ However, strategically the court's indulgence of national security concerns might not be as great in a civil matter. Additionally, the pretrial deposition process of civil litigation might make it harder to control questioning regarding sources and methods underlying the decryption process.

185. The defendant might argue that if the information cannot be linked somehow to the defendant, it might lack sufficient relevance to be admitted into evidence. This objection lacks merit because under Federal Rules of Evidence 901 ("Requirement of Authentication or Identification") and 402 ("Relevant Evidence Generally Admissible; Irrelevant Evidence Inadmissible"), it is only necessary to produce evidence sufficient to support a finding that the item is what its proponent claims it to be and that it is relevant to the case. While defense objections of lack of nexus to the defendant could go to relevance, it is doubtful that a proponent would offer such evidence where there is no provable nexus to the defendant, at least circumstantially; the weight and significance of the nexus would be a jury question.

186. *See* FED. R. EVID. 104(a) ("Preliminary questions concerning . . . the admissibility of evidence shall be determined by the court . . ."); *id.* R. 104(e) ("[Rule 104] does not limit the right of a party to introduce before the jury evidence relevant to weight or credibility."). Once the evidence has been admitted, the government's concern for protecting cryptographic sources and methods continues. Although preliminary questions of admissibility are for the court, not the jury, and may be heard by the court outside of the jury's presence, *id.* R. 104(a), (c), the defense retains the right to cross-examine, before the jury, as to matters going to weight or credibility, *id.* R. 104(e). The reach of such cross-examination into cryptographic sources and methods may stress the Key Theory approach of limiting such inquiry. The government should be prepared to make careful argument and presentation to the trial court, perhaps with an advance motion in limine, concerning distinctions between cross-examination on sources and methods that may be said fairly to go to issues of weight and credibility, versus using cross-examination to probe government sources and methods just for free discovery or information gathering as to it.

187. *See* FED. R. CIV. P. 26(c)(1)(G) (allowing for protective orders requiring "that a trade secret or other confidential research, development, or commercial information not be revealed or be revealed only in a specified way"); *Autotech Tech. Ltd. P'ship v. Automationdirect.com, Inc.*, 237 F.R.D. 405, 414 (N.D. Ill. 2006) (entering an attorneys'-eyes-only protective order to protect confidential trade secret information).

Conclusion

In these ways, the Key Theory offers a process for the government to authenticate decrypted information without exposing sensitive sources and methods. The Key Theory can be used both to protect national security and promote a more efficient litigation process.