PEPPERDINE UNIVERSITY

Pepperdine Law Review

Volume 30 | Issue 2 Article 4

1-20-2003

Double-Clicking on Fourth Amendment Protection: Encryption Creates a Reasonable Expectation of Privacy

Sean J. Edgett

Double-Clicking on Fourth Amendment Protection: Encryption Creates a Reasonable Expectation of Privacy

TABLE OF CONTENTS

I. INTRODUCTION

Personal e-mails, electronic diaries, trade secrets, and other personal data rapidly fill hard drives, network servers, and the Internet. As these private and confidential thoughts continuously pour into electronic form, there is a growing need for electronic security and privacy. Millions of Americans use computers to store their personal, private, and confidential information. Additionally, six out of every ten American households regularly use their access to the Internet to share documents, send e-mails, and research.[1] In this rapidly growing age of cyberspace and electronic document dependency, encryption offers a way to protect files from prying eyes by locking electronic documents and allowing computer users to select who will have the ability to read them. However, while encryption offers a practical way to protect documents in digital form, an erroneous interpretation of encryption's importance, process, and constitutionally relevant factors could effectively delete the need and expectation of privacy that encryption currently offers.

Whether or not encryption is afforded constitutional protection will affect numerous areas of our lives. "In this electronic and digital age, the ability of a speaker and a selected audience to communicate in confidence . . . may be critical to the survival of free speech and privacy."[2] Moreover, in the digital age, there are very few options one can choose from to make a document or communication private. Encryption provides a high level of security and privacy by restricting access to files to only those that have an electronic key.[3] This security option may have myriad effects:

> Cryptography has created new opportunities to protect our private communications and intimate information so that this electronic medium can continue to grow. Industry and commerce can prosper with the assurance that information and trade secrets can be transferred electronically with security. However, the increasing popularity of encryption technology has raised the ire of the government in the name of national security. In an effort to control the rapid growth of cryptography, the government has enacted laws controlling cryptography's development and dissemination. The laws have the effect of inhibiting the free flow of ideas among

1. *See* Amanda Cantrell, *Growth of Internet Access Slows Dramatically in U.S.*, The Industry Standard, *at* http://www.thestandard.com/article/0,1902,28692,00.html (Aug. 27, 2002) and on file with author. According to this survey, it was recently discovered that fifty-eight percent of all Americans had Internet access at home as of July 2001 compared with 52 percent in July 2000 and 39 percent the year before. *Id.*

2. John A. Fraser III, *The Use of Encrypted, Coded and Secret Communications is an "Ancient Liberty" Protected by the United States Constitution,* 2 VA. J.L. & TECH 2, 2 (1997).

3. *See* discussion *infra* Section II.

> people who wish to communicate in this manner. The existing laws remove an entire area of communication from public debate and pose the potential to bar the First Amendment from electronic communication.[4]

As computers continue to network, encryption may be the only way for users to protect their documents and ensure that they control the access to their files. In a sense, encryption offers a cyber-safe where one can store one's digital belongings. Reliance on protections such as individual computer accounts, password protection, and encryption of data should be no less reasonable than reliance upon locks and bolts, even though each form of protection is penetrable.[5]

The sections of this article are divided to provide discrete reasons why encryption is, and should be, protected by law. At the outset, Section II gives a general overview of the encryption process and highlights the power encryption technology.[6] It becomes apparent when understanding the encryption process that utilizing encryption is a considerably reliable way to protect electronic data. Section III offers a historic prospective on the uses of encryption.[7] It demonstrates that the framers of the United States Constitution readily used encryption technology to protect their communications and afford themselves privacy. Section IV defines the evolution of the right to privacy.[8] This section provides a foundation for why the Fourth Amendment's evolution is developing toward protecting encrypted data. Section V specifically responds to an article recently written by Professor Orin Kerr[9], who argues that encrypted data is not constitutionally protected.[10] This section goes through three of the main cases that Professor Kerr cites and discusses why they do not support his proposition when applied to the current uses of encryption and electronic documents. Section V also reveals that the Court might already be on a path to giving encrypted documents privacy protection. Finally, Section VI will explain why the lock-and-key analogy is valid. It will show how the

4. Norman Andrew Crain, *Bernstein, Karn, and Junger: Constitutional Challenges to Cryptographic Regulations*, 50 ALA. L. REV. 869, 870 (1999).

5. Randolph S. Sergent, Note, *A Fourth Amendment Model for Computer Networks and Data Privacy*, 81 VA. L. REV. 1181, 1200 (1995).

6. *See infra* notes 12-31 and accompanying text.

7. *See infra* notes 32-38 and accompanying text.

8. *See infra* notes 39-87 and accompanying text.

9. Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?,"* 33 CONN. L. REV. 503 (2000).

10. *See infra* notes 88-144 and accompanying text.

analogy allows easy translation from the Fourth Amendment protection that the Court has granted physically locked containers to digitally encrypted documents that give rise to a reasonable expectation of privacy.[11]

II. THE ENCRYPTION PROCESS

It is important to understand the process and sophistication of encryption in order to understand the amount of privacy and security that is afforded by this cyber technology. In general, the process of encryption cloaks a document by making it effectively invisible to any computer or person that does not possess the correct encryption key.[12] Once a document is encrypted, it can be transmitted through the Internet, shared with other users over a network, or left on a personal computer, all with the owner of the document having control of exactly who can access the document's contents.[13]

A. Encryption Generally

Encryption works by employing "complex algorithms to mix characters of a message with other characters or values in a seemingly nonsensical way."[14] This results in an electronic file that is "gibberish" to anyone that does not possess the password or encryption key necessary to decode the file.[15] This basic process is employed in storing, transmitting, or creating information in a form that appears hidden from unauthorized users.[16] The plaintext, or original message or document, is "scrambled using a software

---

11. *See infra* notes 145-156 and accompanying text.

12. Andrew B. Berman, *International Divergence: The "Keys" To Signing On The Digital Line—The Cross-Border Recognition Of Electronic Contracts And Digital Signatures*, 28 SYRACUSE J. INT'L L. & COM. 125, 128 (2001) (providing a general overview of the encryption process and its effectiveness to protect documents). For additional information on the encryption process, *see generally* Kerr, *supra* note 9, at 510 (giving a basic overview of the process of encryption and cryptology without focusing specifically on electronic documents and the Internet); James W. Butler, III, *Safe And Legal E-Commerce: Legal and Regulatory Issues Raised by the Use and Export of Encryption Technology*, 611 PRACT. LAW INST. 935, 939-48 (2000) (providing a basic overview of the digital encryption process as it is used by the lay computer user with a good description of encryption vocabulary and computer terms).

13. Berman, *supra* note 12, at 128.

14. Alex Salkever, *Uncle Sam Should Learn to Hack; Banning the export of encryption software won't hamper terrorists' ability to communicate. There are better ways to plumb their secrets,* BUS. WK. ONLINE, Oct. 15, 2001, *available at* 2001 WL 25755236 (arguing that encryption provides a lock-tight method of protecting documents that would take supercomputers hundreds of years to decipher). *See generally* SIMON SINGH, THE CODE BOOK: THE EVOLUTION OF SECRECY FROM MARY, QUEEN OF SCOTS, TO QUANTUM CRYPTOGRAPHY (1999).

15. Salkever, *supra* note 14.

16. *Crypto primer: A Simple Explanation of Encryption*, *at* http://www.techtv.com/callforhelp/features/story/ 0,24330,2001052,00.html and on file with author (Nov. 30, 2001).

application called an encryption engine."[17] The scrambled message is formed when the engine applies additional mathematical data, also called a key, to the plaintext.[18] This scrambled message, called ciphertext, makes a document unintelligible to anyone that does not "have access to the key and decryption software."[19]

B. The Encryption Process

Non-electronic based encryption can be exceedingly simplistic and is far less sophisticated than computer-based encryption used today.[20] However, its process is useful for a basic understanding of how encryption works. Encryption "can be as simple as substituting numbers for letters: A=1, B=2, C=3, and so on."[21] With this simple encryption scheme, an encrypter can provide the code to those people whom the encrypter wants to read the encrypted text.[22] Then, anyone with the code can perform the simple act of substituting the letters in order to figure out the message.[23] However, most modern computers scramble data with such complexity that it is next to impossible to decipher the encrypted document. In fact, it is estimated that, with a sophisticated key encoding system, it would be impossible to decode a document without having a supercomputer work on it for hundreds, or sometimes thousands, of years.[24]

Generally, this sophisticated form of encryption is widely used today in what is called a public key encryption scheme.[25] The system of public key encryption was created to utilize a dual key process: a public key that can be

17. *Id.*
18. *Id.*
19. *Id.*
20. *See id.*
21. *Id.*
22. *Id.*
23. *Id.*
24. NAT'L RESEARCH COUNCIL, CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY 63 (Kenneth W. Dam & Herb S. Lin eds., National Academy Press, 1996) (describing how increasing the key size slightly will increase the time it takes a single computer to decipher a document from a few days to 2,000 years). *See also* Paul Magnusson, *Yes They Certainly Will*, BUS. WK., Nov. 5, 2001, at 90 (noting that a system or document that is protected by a 1,024-bit key code is impossible to break "without a supercomputer working away for a hundred years").
25. *See* George V. Hulme, *Public Key Encryption Algorithm Is Unveiled Early And Promises More Industry Tools*, INFO.WK., Sept 11., 2000, at 39 (outlining the ubiquity of public key encryption in the digital age and its uses in cyberspace); Thomas E. Weber, *World: Looking at Technology That Has the Potential To Thwart Terrorists*, ASIAN WALL ST. J., Sept. 18, 2001, at 7 (noting that the most widely used online encryption systems are public key based).

widely known and even published, and a private key that is needed to unlock the document encoded with the public key.[26] This offers ease to the encryption process and allows many users to encrypt documents. It is important to understand how this type of encryption is used because it is typically the encryption technique used in cyberspace. Consider the following example of how this type of encryption is typically utilized:

> Sam completes a message to Ruth in plaintext form. Upon completion, Sam encodes the message with Ruth's public key. When Ruth receives the message in ciphertext from Sam, she uses her private key to decode the message into plaintext. To send a message back to Sam, Ruth encodes her message with the use of Sam's public key. Sam then uses his private key to decode the message.[27]

In considering this example, it should be noted that the system is extremely secure. This extreme security comes from the fact that the only method of breaking the security of the document is "for either Ruth or Sam to give away their private keys."[28] Moreover, it has been found that "[p]ublic key cryptographic technology has delivered military-grade cryptography with the level of security so high that even the ultra-secret, code-breaking computers at the National Security Agency cannot decipher the encrypted messages."[29]

C. The Importance of "The Key"

An encryption key provides a unique code that keeps a file protected, making the key the most important part of the process. The strength of a coded communication is dependent upon the key, and not the algorithm used to encode the message.[30] Knowledge of the algorithm is worthless without the key—the key is the only thing that can decrypt the message—so it does not matter if everyone is using the same algorithm.[31] This becomes important when understanding why the digital encryption process works like a typical lock and key in the physical world.[32]

---

26. Crain, *supra* note 4, at 872.
27. *Id.* (internal citations omitted).
28. *Id.*
29. *Id.*
30. *Id.* at 872.
31. *See id.*
32. *See infra* notes 12-30 and accompanying text.

It is essential to keep this description of the encryption process in mind when evaluating whether or not the entire process seems to create a reasonable expectation of privacy, which will result in a legal protection of encrypted documents. Analyzing case law with this explanation of encryption in frame will demonstrate that courts may be on the path to finding that encrypting documents creates Fourth Amendment protection. In addition, history surrounding the formation of the constitution demonstrates that the framers started the legal path of search and seizure protection while using encryption technology. Extending the understanding of encryption to the physical world allows for an analogy with a traditional lock and key mechanism. All of this will provide some insight into how the courts will rule on encrypted documents.

III. THE FOUNDERS AND ENCRYPTION

Encryption has been used for centuries as a way to keep documents and communications private.

> Constitutional analysis of issues arising from encryption technology must proceed from the understanding that the generation of actors that framed the Constitution and the Bill of Rights were sophisticated users of secret communications, and that they used secret communications to protect and advance the political objectives that they most valued.[33]

The Founders used secret communication methods like encryption (then a basic cryptology scheme) to hide information from those not intended to receive the information and to act as a "secure seal."[34] Encryption was widespread and used essentially to "seal" documents and discussions that were being communicated.[35] It has been recently discovered that many historic figures used encryption in communications when they intended the

33. Fraser, *supra* note 2, at 2. *See also*, Ryan Alan Murr, Comment, *Privacy and Encryption in Cyberspace: First Amendment Challenges to ITAR, EAR and Their Successors*, 34 SAN DIEGO L. REV. 1401, 1461 (1997). Murr argues that the Framers were proponents of secret communications and conversations in private. *Id.* He believes that we should analogize encryption to a "digital whisper" and see that it is exactly what the Framers were doing during the time they created the constitution. *Id.*

34. RALPH E. WEBER, UNITED STATES DIPLOMATIC CODES AND CIPHERS, 1775-1938 (1979).

35. *See id.*

highest amount of privacy.[36] From this, it can be inferred that the Founders recognized the great privacy and security encryption afforded its users.

American history has accordingly demonstrated that citizens have long enjoyed the use of encryption and other forms of secret writings.[37] It has only been in the last three decades that the government has had the ability to decipher these writings.[38] It seems that while the Founders were afforded the use of encryption to protect their documents, it should not be the case that recent technology should evaporate this technique of keeping things private. While there is no direct evidence to prove that the founders were specifically thinking of encryption as something to be protected against government intrusion, it should be recognized that encryption is an ancient liberty.[39]

IV. THE RIGHT TO PRIVACY HISTORICALLY AND MODERNLY DEFINED

The Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[40] "The requirement to turn over one's encryption key, a *priori* and without any prior showing of probable cause to believe criminal conduct has taken or will take place, would seem to implicate this most fundamental concern of the Fourth Amendment."[41] However, does Fourth Amendment protection really protect digital media that have been encrypted? A look into original cases of privacy may illustrate the answer.

---

36. *See, e.g.*, THE ADAMS FAMILY PAPERS, SERIES II, ADAMS FAMILY CORRESPONDENCES, 162-63 (L.H. Butterfield ed., 1973).

37. *Id.*

38. Fraser, *supra* note 2.

39. *Id.*

40. U.S. CONST. amend. IV.

41. David B. Walker, *Privacy in the Digital Age: Encryption Policy—A Call for Congressional Action*, 1999 STAN. TECH. L. REV. 3, 44 (1999). Walker argues "[t]he real threat to privacy interests is that the courts will misapprehend the nature of the technology and will therefore miscategorize key escrow to place it outside the ambit of the Fourth Amendment." *Id.*

A. Olmstead v. United States[42]*: History in Transition*

The right to privacy was initially stated, in *Olmstead v. United States,* in terms of the right to be left alone.[43] In that case, federal agents installed wiretaps in the basement of a suspected bootlegger's building and obtained a conviction with evidence obtained from the wiretaps' recordings. Although the majority stated that a party's Fourth Amendment rights could not be infringed because the wiretapping did not constitute a search and seizure under the meaning of the Fourth Amendment, dissenting Justice Brandeis feared that if the government were allowed to break the law like it did in this case, it would invite every person to break the law and would result in anarchy.[44]

Brandeis believed that invading the privacy of an electronic communication was a far greater attack on privacy than the government invading the privacy of a person's mail.[45] At the time of the case, mail was afforded privacy protection under the Fourth Amendment.[46] Thus, in order to protect the right to privacy, Justice Brandeis asserted that every intrusion made by the government on someone's private life should be deemed a violation of the Fourth Amendment. This policy of Fourth Amendment privacy was later adopted in the Court's history in *Katz v. United States.*[47]

---

42. 277 U.S. 438 (1928).

43. *Id.* at 478 (Brandeis, J., dissenting). The dissent believed that the most important right valued by American citizens is the right to be left alone. *Id.* In order to protect this right, "every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment." *Id.* It is significant to note that Justice Brandeis actually was referring to the telephone as a form of electric communication. He stressed the importance of protecting electronic forms of communication, which could be seen as comparable to digital documents. *See Ex parte* Jackson, 96 U.S. 727 (1877) (arguing that no difference exists between a sealed mailed letter and a private telephone or electronic message).

44. *Olmstead,* 277 U.S. at 485. Justice Brandeis is advocating the Court's recognition of a right to privacy and relying on the philosophical values motivating the Fourth Amendment. *See also* R. Brian Black, *Legislating U.S. Data Privacy in the Context of National Identification Numbers: Models from South Africa and the United Kingdom,* 34 CORNELL INT'L L. J. 397, 414 (2001) (stating that Justice Brandeis is focused on the desire to protect citizens from government interference).

45. *Olmstead,* 277 U.S. at 475.

46. *See id.*

47. 389 U.S. 347 (1967). In *Katz,* the lower court followed the holding in *Olmstead* and rejected the defendant's claim that his Fourth Amendment rights were violated because the government had not physically entered an area occupied by the defendant. Mark Elmore, *Big Brother Where Art Thou, Electronic Surveillance and the Internet: Carving Away Fourth Amendment Privacy Protections,* 32 TEX. TECH. L. REV. 1053, 1059 (2001). It is paramount to note that in overturning *Olmstead, Katz* erased a longstanding rule that Fourth Amendment protection only extended to physical breaking and entering. This overturning affords an extension of the ruling to electronic

B. Katz v. United States[48]*: The Modern Approach*

In *Katz*, the Court adopted Justice Brandeis's dissent and extended the right of privacy to circumstances where the government did not physically intrude on someone's private space.[49] In the case, federal agents attached an electronic listening and recording device to the outside of a public phone booth in the belief that the defendant used the booth to transmit wagering information by telephone.[50] The government, through this wiretapping, found that Katz was transmitting wagering information via telephone, and Katz was convicted.

Moving away from its tradition of requiring physical intrusion, the Court held that Katz was entitled to Fourth Amendment protection for his conversations and that a physical intrusion into the area he occupied was not necessary to invoke the Amendment's protections.[51] The Court rejected the legal theory that Fourth Amendment protection extends only to constitutionally protected areas.[52] In place of this theory, the Court recognized that the Fourth Amendment protected people and not specific places.[53] The Court stressed that it is imperative to understand where and when someone has a reasonable expectation of privacy. It stated that the Fourth Amendment "protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all."[54] But what creates these privacy interests?

The Court recognizes that seeking to exclude someone from an area (in this case, excluding others from hearing a conversation) is the starting point on the road to creating a reasonable expectation of privacy.[55] "[We] have expressly held that the Fourth Amendment governs not only the seizure of tangible items, but extends as well to the recording of oral statements, overheard without any 'technical trespass under . . . local property law.'"[56] Additionally, the Court held that just because an "electronic device employed to achieve that end did not happen to penetrate the wall of the

---

communication, where many do not see a "physical intrusion."

48. 389 U.S. 347 (1967).

49. *Id. Katz* was the first time the Court did not require there to be a physical entry in order to make a claim for Fourth Amendment protection. Jennifer Mulhern Granholm, *Video Surveillance on Public Streets: The Constitutionality of Invisible Citizen Searches*, 64 U. DET. L. REV., 687, 691 n. 24 (1987).

50. *Katz*, 389 U.S. at 348.

51. *Id.* at 354-59.

52. *Id.* at 350.

53. *Id.* at 361 (Harlan, J., concurring).

54. *Id.* at 350.

55. *Id.* at 352.

56. *Id.* at 353.

booth can have no constitutional significance."[57] Justice Harlan concurred and constructed what would become the current test of what is constitutionally protected as "private": whether someone had a reasonable expectation of privacy.[58]

Justice Harlan, in his concurring opinion, came up with a two-part test that is currently used to determine whether there is a reasonable expectation of privacy as to create the need for a warrant for government entry.[59] The test requires one to ask whether there is a subjective expectation of privacy and whether that subjective expectation of privacy is one that "society is prepared to recognize as 'reasonable.'"[60]

As a result, "[t]he scope of the modern Fourth Amendment is based upon whether a reasonably held expectation of privacy has been violated, and not upon the place invaded or even the meanings of the word 'search.'"[61] "'[T]he Court now uses the notion of... a 'legitimate expectation of privacy'... to identify, at least in part, those interests protected by the Fourth Amendment. If no such expectation is invaded, it is generally said that no 'search' has occurred.'"[62] On the contrary, when a reasonable expectation of privacy is found, then the Fourth Amendment is activated and a warrant is necessary to conduct a search.[63] As long as a

57. *Id.* This passage is extremely relevant to encryption technology. The Court stated that no physical entry has to occur, and there does not have to be a physical barrier protecting a private area. This is similar to encryption where there is only a digital protection, and invading the encrypted document does not require any physical invasion. It could be argued that encryption does not penetrate or break anything. Kerr, *supra* note 9, at 520-24. The Court has moved away from the property law concept of invasion and has expanded the doctrine to include electronic communications. Bartnicki v. Vopper, 532 U.S. 514 (2001) (protecting the privacy interest of a cellular phone conversation). It began to completely move away from the property law doctrine of trespass in *Silverman v. United States*, 365 U.S. 505 (1961) (holding that audio surveillance through a wall is a violation of Defendant's Fourth Amendment right to privacy). The Court has continued this trend with *Katz*.

58. *Katz*, 389 U.S. at 360. The Court, however, has never said what exactly constitutes a "reasonable expectation of privacy." It has, nevertheless, laid down some factors to be considered when determining a privacy right: intention of the Framers of the Fourth Amendment, *United States v. Chadwick*, 433 U.S. 1, 7-8 (1977); the ways in which the individual has used a location, *Jones v. United States*, 362 U.S. 257, 265 (1960); and our societal understanding that certain areas deserve the most protection from government invasion, *e.g.*, *Payton v. New York*, 445 U.S. 573 (1980).

59. *Katz*, 389 U.S. at 360-62 (Harlan, J., concurring). This test is later adopted by the majority in *Terry v. Ohio*, 392 U.S. 1, 9 (1968).

60. *Katz*, 389 U.S. at 361.

61. Timothy B. Lennon, Comment, *The Fourth Amendment's Prohibitions on Encryption Limitation: Will 1995 Be Like 1984?*, 58 ALB. L. REV. 467, 482 (1994) (citing *Katz*, 347 US at 350).

62. *Id.* (citing Peter Goldberger, *Consent, Expectations of Privacy, and the Meaning of "Searches" in the Fourth Amendment*, 75 J. CRIM. L. & CRIMINOLOGY 319, 322 (1984)).

63. *See id.*

reasonable expectation of privacy exists in a communication, an infringement upon that expectation will require adherence to the Fourth Amendment.[64]

C. Specific Application of the Reasonable Expectation of Privacy Rule to Encryption

It can be argued that encryption provides the same expectation of privacy as the expectation acknowledged in *Katz*. This is because the Court has held that when a person takes affirmative steps to ensure that their property remains private, an expectation of privacy is created that is equal to the protection that exists in one's locked briefcase, home, or trunk.[65] The process of encryption creates protection that is parallel—if not better—than the protection that exists with a locked box or sealed envelope.[66] Because digital encryption works to ensure that the individual encrypting the document can control access to the document, just like a locked container, a sense of complete privacy exists.[67]

This sense of complete privacy when encrypting a document should be seen as an affirmative step aimed at creating a reasonable expectation of privacy. Those that actually encrypt their documents are taking affirmative steps above and beyond the steps taken by regular computer users. Those that encrypt are attempting to ensure that their documents will remain secure by building an electronic safe around their electronic property. As a consequence, it can be argued that someone that encrypts is exhibiting an actual expectation of privacy in relation to specific documents that he or she

---

64. *Id.*

65. These affirmative steps have to satisfy the two-part test from *Katz* and *Terry*. The Court has determined that locking a box can create a reasonable expectation of privacy—"[a] container which can support a reasonable expectation of privacy may not be searched, even on probable cause, without a warrant." United States v. Jacobsen, 466 U.S. 109, 120 n.17 (1984). The Court has also determined that there is a reasonable expectation in a locked footlocker, and that there is not a reduced expectation of privacy in that footlocker just because it is in public view. United States v. Chadwick, 433 U.S. 1, 11 (1977). "Respondents principal privacy interest in the footlocker was, of course, not in the container itself, which was exposed to public view, but in its contents." *Id.* at 13-14 n.8.

66. *See generally supra* notes 12-31 and accompanying text on the process of encryption. The Court has determined that "[l]etters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy; warrantless searches of such effects are presumptively unreasonable." United States v. Jacobson, 466 U.S. 109, 114 (1984). The Court has held that there can be a reasonable expectation of privacy in a storage locker, *United States v. Karo*, 468 U.S. 705, 721 (1984); in closed luggage, *Robbins v. California*, 453 U.S. 420, 434 n.3 (1981); and in a double-locked footlocker, *United States v. Chadwick*, 433 U.S. 1, 11 (1977).

67. Jim Nesbitt, *Keeping it Confidential: Taking Charge of Internet Privacy*, SAN DIEGO UNION-TRIBUNE, May 30, 2000, at Computer Link 1 (arguing that "[e]ncryption can be used to regain [a] sense of privacy and the sense of control over the information."); Peter Lunt, *The Electronic Consumer: www.confidence*, CONSUMER POLICY REVIEW, Nov. 1, 1999, at Vol. 9, Iss. 6.

encrypts. It does not seem any more reasonable to place an object in a sealed envelope or lockbox than it does to digitally encrypt the object to make it just as invisible to the naked eye.[68] If encryption is denied the constitutional protections that are afforded to locked boxes, then an illogical requirement for search and seizure protection will be created: computer users are going to need to print out their digital documents and then lock them in a safe. This would seem counterintuitive.

D. Rights-based Conceptions of the Fourth Amendment: Current Exceptions do not Exempt Encryption from Fourth Amendment Protection

Over time the Supreme Court has carved out a number of exceptions to the rights-based expectation of privacy. In a number of well-cited cases, the Court has maintained that a mere expectation of privacy does not necessarily mean that there is a recognizable constitutional privacy interest.[69] The Court looks to a rights-based approach to analyze whether or not there was a reasonable expectation of privacy.[70] In each of its cases, the Court has dismissed a statistical approach to claiming that a right to privacy is present.[71] Moreover, the Court has held that just because it is statistically reasonable to believe that activities or substances will remain private does not mean that there is a constitutionally protected interest of privacy in those activities or substances.[72] In each landmark case, the Court defines exceptions that should not mistakenly be translated into a formula that makes encryption a constitutionally unprotected means of privacy.[73]

---

68. According to the Court, placing a document in a safe or envelope does create a reasonable expectation of privacy. United States v. Jacobson, 466 U.S. 109, 115 (1984).

69. *See* United States v. Jacobson, 466 U.S. 109 (1984); United States v. White, 401 U.S. 745 (1971) (holding that the use of agents who themselves may reveal the contents of conversations with an individual does not violate a Fourth Amendment right to privacy); United States v. Miller, 425 U.S. 435 (1976) (holding that the Fourth Amendment does not prohibit the government from obtaining confidential information from third-parties who the accused was statistically reasonable in believing would not tell anyone else).

70. *See generally* Kerr, *supra* note 9, at 507 (arguing that an "expectation is constitutionally reasonable or 'legitimate' when it is backed by an enforceable, extraconstitutional right to enjoin the government's invasion of privacy").

71. *See, e.g.*, Florida v. Riley, 488 U.S. 445 (1989) (White, J., plurality) (holding that viewing the defendant's greenhouse from a low-flying helicopter was not a search because the fact that it was statistically improbable for someone to fly over in a helicopter it did not mean that there was a reasonable expectation of privacy).

72. *Id.*

73. *See, e.g.*, *Jacobsen*, 466 U.S. at 109; *Riley*, 488 U.S. at 445.

In *United States v. Jacobsen*, the appellant complained that the field test conducted on the cocaine he possessed when he was searched violated his Fourth Amendment right because of his belief that the contents of the powder would remain secret.[74] In response to this, the Court held that the field test merely determined whether or not the particular substance was cocaine, and did not compromise any legitimate interest in privacy.[75] The Court noted that cocaine is an illegal matter and that the field test destroyed only a trace amount of the substance.[76] From this, it could be argued that decoding an encrypted document does nothing to destroy its contents and thus, under *Jacobsen*, there is no unconstitutional search or seizure. However, this argument is defective.

The Court's holding in *Jacobsen* does not apply to deciphering encrypted documents. Unlocking an encrypted document is like breaking open a locked box and then searching its contents.[77] If the government is in possession of an encrypted, locked document, the government will have to break apart the document with a supercomputer to see its contents.[78] The encryption process could be analogized to *Jacobsen:* just as none of the cocaine was lost in the field test, encryption does not destroy any physical properties. Nevertheless, in cyberspace this would be like breaking open a box. Just because there is the possibility of digital reassembly does not mean that there is no expectation of privacy.[79]

In *Florida v. Riley,* a defendant growing marijuana in his backyard attempted to ensure that no one knew of the illegal activity by building a fence and modest covering over the marijuana so it could not be seen from the street.[80] The government flew a helicopter over the property and discovered the drugs in the greenhouse.[81] The defendant complained that he had a reasonable expectation of privacy in the enclosed area and that the

74. *Jacobsen*, 466 U.S. at 112.

75. *Id.* at 122-23.

76. *Id.* at 125.

77. In cyberspace, while the encrypted document can be "repaired" once it is deciphered by re-encrypting it, the analogy fails. This is analogous to saying that it is okay to break open a locked box because it can be put back together again.

78. The word "break" in this context is used in a cyber sense, where entering into a document would be like entering into an envelope in the physical world—there would have to be a break.

79. I plan to flesh out this argument by demonstrating that encryption creates a virtual lockbox around the contents of the document. Furthermore, making the argument that just because nothing is really lost when the file is deciphered would mean that nothing in cyberspace could be protected since there could really be no "breaking and entering."

80. Florida v. Riley, 488 U.S. 445, 445 (1989) The Court, while upholding an aerial search, noted that police did not observe any intimate details during the search. *Id.* at 452. The Court noted that if the helicopter had been flying at an illegal altitude, then a different result would have been achieved. *Id.* at 451.

81. *Id.* at 448.

government should have procured a warrant before flying over.[82] In considering this claim, the Court responded that the government could go anywhere that is legally accessible to the public.[83] In addition, it found that there is no reasonable expectation of privacy in areas that can be viewed or legally accessed by the public.[84] The Court noted that while the defendants could have rationally expected their fences and structure to create privacy around their drugs, no law or recognized social practice allowed the defendants to enjoin law enforcement from entering public space in a helicopter in order to view the land below it—it is an activity that anyone can participate in.[85]

The holding of this case can be used to argue that while there is a social practice—albeit a very narrowly defined one amongst users of encryption and computers—that encryption creates a reasonable expectation of privacy, it is a case of misplaced confidence. *Riley* demonstrates that when someone mistakenly believes that he is working in a private area that can be seen by no one else or where no one else will reveal the secrets he has told them, his beliefs are not controlling where there is no complete privacy (like the area viewable by the helicopter).[86] But encryption is functionally different from this case. Encryption is not an open field—it is a completely sealed digital

82. *Id.* at 451-52.

83. *Id.* at 449 (quoting California v. Ciraolo, 476 U.S. 207, 213 (1986)). However, just because something. is accessible to the public does not mean that there cannot still be a reasonable expectation of privacy. United States v. Oliver, 466 U.S. 170, 171 (1984). Courts have extended the *Katz* doctrine to include areas that could possibly be visible by the public eye. *See, e.g.*, United States v. Mullinex, 508 F. Supp. 512, 514 (E.D. Ky. 1980) (holding that a person may have an expectation of privacy in an open field if society would consider it reasonable); United States v. DeBacker, 493 F. Supp. 1078, 1080-81 (W.D. Mich. 1980) (holding that the government should not be given carte blanche to search areas outside the curtilage as a matter of course); Dean v. Superior Court, 110 Cal. Rptr. 585, 589 (1973) (finding that the *Katz* reasonable expectation of privacy test is more appropriate because the open fields doctrine is reminiscent of a constitutionally protected areas approach); State v. Brady, 406 So. 2d 1093, 1096 (Fla. 1981) (holding that the open fields doctrine may receive Fourth Amendment protection if it passes both prongs of the *Katz* test). When arguing that *Riley* is applicable to encryption, it should be noted that there are myriad exceptions that seem to trace back to the primary test of *Katz*: whether society deems it reasonable to have an expectation of privacy in a particular area.

84. *Riley,* 488 U.S. at 449.

85. Kerr, *supra* note 9, at 510 (internal citations omitted). *See also,* California v. Ciraolo, 476 U.S. 207, 213-14 (1986) (finding the observation of a backyard from a plane in public airspace to be permissible despite six foot outer fence and ten foot inner fence around backyard because the property was still viewable from areas of public access).

86. *See, e.g.*, Hoffa v. United States, 385 U.S. 293, 302 (1966) (holding that individuals cannot rely on their confidence that co-participants in illicit activities will not disclose their crimes); Lewis v. United States, 385 U.S. 206, 210 (1966) (finding no Fourth Amendment violation when defendant invited an undercover agent into his home to buy narcotics).

area that cannot be viewed by anyone without a key. The confidence and reliance on the privacy aspect of encryption is not "misplaced." In the cyber world, it is the physical equivalent of a steal, sealed box.[87]

V. WHY ENCRYPTION SUCCEEDS IN CREATING A REASONABLE EXPECTATION OF PRIVACY WHERE OTHER "ENCODINGS" FAIL: AN ANALYSIS OF CASE LAW

The encryption process locks a document and keeps it safe from intruding eyes by affording significant security features. Supercomputers sometimes require hundreds or thousands of years to decrypt a document. Moreover, a document's owner can control who can see the document's content, and without deciphering an encrypted document it is virtually invisible.[88] It seems that with all of the protections encryption provides, courts will find that encryption provides a reasonable expectation of privacy that is protected under the Fourth Amendment. However, it might be argued that federal and state case law demonstrates that courts will not be willing to give encryption Fourth Amendment protection.

In a recently published journal article, Professor Orin Kerr argues that three noteworthy cases that apply the reasonable expectation standard demonstrate that encryption fails to satisfy a constitutionally protected method of privacy.[89] This section attempts to analyze the same three cases that Kerr cites in order to demonstrate that encryption in cyberspace can be found by the court to be in the purview of the Fourth Amendment. All three cases demonstrate situations where "coding" efforts failed to provide a reasonable expectation of privacy. The courts' reasoning is essential to understanding why digital encryption is not comparable to these three specific situations and to understanding how digital encryption provides what the courts say is lacking to create a reasonable expectation of privacy.

---

87. *See supra* notes 12 -31 and accompanying text for discussion of encryption and power of the encryption key. This analogy comes from the fact that the encryption locks a document in a fashion that requires someone who wants to view it to have an encryption key—similar to a locked box or trunk. It takes most computers hundreds or thousands of years to view an encrypted document without this encryption key.

88. *See supra* notes 12-31 and accompanying text on the process of encryption.

89. Kerr, *supra* note 9, at 513-17. Orin Kerr is a professor at George Washington University School of law. He has served as a trial attorney in the Computer Crime and Intellectual Property Section of the Criminal Division at the U.S. Department of Justice. Professor Kerr developed special expertise in computer search and seizure and electronic privacy law. Information on Professor Kerr is available at http://www.law.gwu.edu/fac/faculty.asp?pkey_f=96.

A. United States v. Longoria[90]

In *Longoria*, members of a narcotics conspiracy "encoded" their communications by speaking in Spanish when they were around non-conspirators.[91] Thinking that the other people could not understand Spanish, the coconspirators spoke openly about their illegal plans.[92] Mistakenly, however, they discussed their plans to conduct drug transactions in the presence of a government informant who recorded the conversation and later translated it into English.[93] Defendants argued that they had a reasonable expectation of privacy in their communications because they were encoded in Spanish.[94] The court rejected the defendant's argument in *Longoria* and stated that there is no constitutionally reasonable expectation of privacy in these clearly audible conversations.[95] "[O]ne exposing conversations to others must necessarily assume the risk his statements will be overheard *and* understood."[96] The defendant "exposed his statements by speaking in a manner clearly *audible* by the informant. His hope that the informant would not fully understand the contents of the conversation is not an expectation 'society is prepared to recognize as reasonable.'"[97]

---

90. 177 F.3d 1179 (10th Cir. 1999). The court focused on the two part test to determine whether a defendant has a reasonable expectation of privacy if: "(1) the defendant had an actual, subjective expectation of privacy—i.e., that his communications were not subject to interception; and (2) the defendant's expectation is one society would objectively consider reasonable." *Id.* at 1181-82.

91. *Id.* at 1183.

92. *Id.* at 1181.

93. *Id.*

94. *Id.* at 1182. The defendant did not make an "encoding" argument, but stated that he "did not 'knowingly expose' his conversations to the informant because he spoke in a language he believed the informant could not understand." *Id.* at 1183. It could be argued that this is similar to encryption, because it creates a language that can only be understood by one who knows the language, essentially the one who has the encryption key.

95. *Id.* at 1184.

96. *Id.*

97. *Id.* at 1183 (quoting Katz v. United States, 389 U.S. 347, 361 (1961) (Harlan, J. concurring)). *See also* Siripongs v. Calderon, 35 F.3d 1308, 1320 (9th Cir.1994) (concluding that a defendant had no expectation of privacy in conversations conducted in Thai in the presence of a police officer); *In re* Matter of John Doe Trader Number One, 894 F.2d 240 (7th Cir. 1990) (holding that a defendant had no reasonable expectation of privacy in conversations conducted on trading floor in presence of government agent); United States v. Coven, 662 F.2d 162, 173 (2d Cir. 1981) (holding that a defendant had no reasonable expectation of privacy in conversations conducted in informant's presence).

Kerr uses this case to argue that the coding that occurs in encryption is similar to the coding of English to Spanish.[98] Thus, applying the reasoning of *Longoria*, encryption is not protected under the Fourth Amendment.[99] He recognizes that the court said that there was no expectation of privacy in speaking in a foreign tongue, even when you have knowledge that the other people in the room do not understand the language.[100] Utilizing this case, encryption does not create a reasonable expectation of privacy when you analogize foreign language with encryption where someone is trying to protect a communication by making it incomprehensible to anyone else.[101] However, this argument is flawed in its comparison and does not create a prototypical use of encryption in the digital world.

Encryption encodes a digital document and leaves the user with only the key. The Court has determined that this kind of restricted access creates a reasonable expectation of privacy.[102] Utilizing Spanish as a mode of encryption can be analogized to the digital forms, only allowing over 300 million people—the number of Spanish speakers in the world—to have the key.[103] Accordingly, it seems, the court was right in saying that there is no reasonable expectation of privacy from encrypting a communication in a globally spoken language. However, encryption does not work like an international language.[104] There is only one code that can decipher the

98. *See* Kerr, *supra* note 9, at 513-17. Kerr states, "[I]n [*Longoria, Scott,* and *Copenhefer*] the police officers recovered the secret communications, and the defendants argued that the government's actions violated their 'reasonable expectation of privacy' because a reasonable person would have expected that their secrets would remain safe." *Id.* at 513. The foundation for his argument that these cases apply to encryption is that "in all three cases, the courts rejected the defendants' claims and held that decoding the defendants' communications without a warrant did not violate the Fourth Amendment." *Id.*

99. *Id.*

100. *Id.* at 515-16 (citing *Longoria*, 177 F.3d at 1183-84).

101. *See id.* at 515-16.

102. *See, e.g.*, United States v. Ross, 456 U.S. 798, 801, 822-23 (1982) (arguing that the Fourth Amendment "provides protection to the owner of every container that conceals its contents from plain view" and suggesting that a warrant would have been required to search a "'lunch-type' brown paper bag" and a "zippered red leather pouch" had they not been found in an automobile); United States v. Jacobsen, 466 U.S. 109, 111, 114-15 (1984) (suggesting that a warrantless search of an "ordinary cardboard box wrapped in brown paper" would have violated the Fourth Amendment had a private party not already opened it); United States v. Chadwick, 433 U.S. 1, 11 (1977) (asserting that there is a reasonable expectation of privacy in the contents of a 200-pound "double-locked" footlocker); Arkansas v. Sanders, 442 U.S. 753, 762-63 n.9 (1979) (noting that there is a reasonable expectation of privacy in a small, unlocked suitcase); Robbins v. California, 453 U.S. 420, 428-29 (establishing that there is Fourth Amendment protection in packages wrapped in green opaque plastic).

103. Rodrigo Lara Serrano, *Muzo: Hay in Argentin en Misopa*, I. BIZ, Apr. 2000, at 53 (stating that there are more than 388 million Spanish-speakers in the world). In 1999, the Summer Institute for Linguistics Ethnologue Survey estimated there to be 332 million Spanish speakers in the world. *at* http://www2.ignatius.edu/faculty/turner/worldlang.htm and on file with author (last visited Sept. 1, 2002).

104. *See supra* notes 12-31 and accompanying text on encryption process.

message and not 300 million of them that can be used. If individuals are speaking a language unique to the two of them—an equivalent to encryption—then there should be a reasonable expectation of privacy.

There is another reason why analogizing this foreign language case to encryption is invalid: the court focused on the fact that the defendants assumed the risk when they were transmitting conversations in locations inhabited by others.[105] In the typical encryption situation, the only person to see the document is the user, and the transmission happens completely in the confines of the computer. It seems that encryption is exceptionally different than spoken language in this way. Thus, an extension of *Longoria* to say that encryption also is not constitutionally protected is tenuous at best. It is significant that the court notes that the communication would be protected if it passed the two-part test.[106]

B. United States v. Scott[107]

In *Scott*, the defendant shredded evidence of his income tax evasion and placed those shredded documents in the trash.[108] After searching through the trash, the government seized these documents and reconstructed them to their original form.[109] The defendant argued that he had a reasonable expectation in shredded documents because once they were shredded they became virtually unreadable to anyone else.[110] The court rejected this argument completely,[111] finding that there is no expectation of privacy in anything thrown into the garbage.[112] Aside from basing the case on a theory of abandonment, the court also noted that the police can use technology to decode "secret messages." "There is no constitutional requirement that police techniques in the detection of crime must remain stagnant while those intent on keeping their nefarious activities secret have the benefit of new knowledge."[113] The court stressed:

105. United States v. Longoria, 177 F.3d 1179, 1184 (10th Cir. 1999).
106. *Id.*
107. 975 F.2d 927 (1st Cir. 1992).
108. *Id.* at 928.
109. *Id.*
110. *Id.*
111. *Id.* at 931.
112. *Id.* at 929. "In our view, a person who places trash at a curb to be disposed of or destroyed by a third person abandons it because '[i]mplicit in the concept of abandonment is a renunciation of any reasonable expectation of privacy in the property abandoned.'" *Id.* (quoting United States v. Mustone 469 F.2d 970, 972 (1st Cir. 1972)).
113. *Id.* at 930.

> A person who prepares incriminatory documents in a secret code . . . and thereafter blithely *discards them as trash*, relying on the premise or hope that they will not be deciphered . . . cannot make a valid claim that his subjective expectation in keeping the contents private by use of the secret code [or language] was reasonable in a constitutional sense.[114]

However, the court's rationale is conjunctive: the holding was based on the fact that the defendant shredded the paper *and* threw the "secret code" into the garbage.[115] Courts have had a longstanding history of discharging all Fourth Amendment protection from anything thrown into the garbage.[116] As a consequence, *Scott* does not translate into a holding that strikes down constitutional protection from encrypted documents.

But Kerr extends the holding of this case and states that its rationale is applicable to encryption.[117] His analogy maintains that shredding a document into unrecognizable pieces is like encryption.[118] Nevertheless, even if this analogy were correct, it would only illustrate a rule in situations where a document "encoder" throws away encoded documents.[119] Many cases have held that placing objects in the trash extinguishes your reasonable expectation of privacy in the objects.[120] *Scott* just extends that abandonment proposition. It merely shows that if an encrypted document is thrown in the trash, then that document loses Fourth Amendment protection—there is no

---

114. *Id.* (emphasis added) (internal punctuation omitted).

115. *Id.*

116. California v. Greenwood, 486 U.S. 35, 40-41 (1988) ("[H]aving deposited their garbage in an area particularly suited for public inspection and, in a manner of speaking, public consumption, for the express purpose of having strangers take it . . . respondents could have had no reasonable expectation of privacy in the inculpatory items that they discarded." (quoting United States v. Reicherter, 647 F.2d 397, 399 (Cal. 3rd 1981))). *See also* United States v. Dunn, 480 U.S. 294, 304 (stating that an erection of ranch type fences in an open field does not create a constitutionally protected privacy interest); United States v. Wilkinson, 926 F.2d 22, 27 (1st Cir. 1991) (placing trash bags within barrels inside defendant's lawn not entitled to elevated "expectation of privacy" respecting the trash).

117. Kerr, *supra* note 9, at 513-15.

> "In all three cases, the police officers recovered the secret communications, and the defendants argued that the government's actions violated their 'reasonable expectation of privacy' because a reasonable person would have expected that their secrets would remain safe. In all three cases, the courts rejected the defendants' claims and held that decoding the defendants' communications without a warrant did not violate the Fourth Amendment."

Id. at 513.

118. *See id.*

119. *See Scott*, 975 F.2d at 930.

120. *See supra* note 116 (discussing the trash-abandonment theory) and specifically California v. Greenwood, 486 U.S. 35, 35 (1988) (holding that the "Fourth Amendment does not prohibit the warrantless search or seizure of garbage left for collection outside the curtilage of a home").

indication from this case that encryption does not have Fourth Amendment protection.[121]

While the court does note that law enforcement should not have to sit idle to the invention of new technology, the paper-shredding technique by nature creates less privacy than digital encryption. Unlike paper shredding, digital encryption makes it impossible to read a document.[122] While it could be argued that the court is saying that the police should be able to keep up with the encryption techniques and use them to decipher anything, this is missing the court's main point: because the defendant threw his encrypted document in the trash, he no longer could expect it to be kept safe.[123] He effectively discharged his reasonable expectation of privacy when he threw away the shredded documents.[124] To support this argument, a number of cases have held that Scott was decided on a strict abandonment theory.[125]

C. Commonwealth v. Copenhefer[126]

In *Commonwealth v. Copenhefer*, Copenhefer was convicted of kidnapping and murder after police conducted a search of his home during a murder investigation.[127] During the search, the government seized Copenhefer's computer pursuant to a valid search warrant.[128] Once in its possession, the government used computer software designed to retrieve files previously deleted and recovered files that Copenhefer believed he had destroyed.[129] These files contained inculpatory evidence linking Copenhefer

121. *See Scott*, 975 F.2d at 927-31.

122. *See supra* notes 12-31 and accompanying text.

123. *See Scott*, 975 F.2d at 929-30.

124. *Id.*

125. *See* United States v. Redmon, 138 F.3d 1109, 1131 (7th Cir. 1998) (noting that the abandonment theory was used in *Scott*); State v. DeFusco, 620 A.2d 746 (Conn. 1993) (noting that *Scott* argued that just because one shreds his trash doesn't mean he has any different expectation of privacy in it than regular trash). *See also* A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 823-26 (1995). Froomkin argues that "Fourth Amendment privacy in this context begins with the premise that people have control over who knows what about them and 'the right to shape the 'self' that they present[] to the world. This control is protected by the Fourth Amendment freedom from unlawful searches and seizures.'" *Id.* at 826 n. 496. (citing LAURENCE H. TRIBE, AMERICAN CONSTITUTIONAL LAW § 12-1 (2d ed. 1988)).

126. 587 A.2d 1353 (Pa. 1991).

127. *Id.* at 1354-55.

128. *Id.* at 1355.

129. *Id.* at 1356.

to murder and kidnapping.[130] Copenhefer argued that the government's seizure of the electronic documents that he believed he had deleted from his computer constituted an impermissible violation of his Fourth Amendment rights.[131] He contended that he had a reasonable expectation of privacy in the files because he thought he had destroyed them and had a "hope of achieving secrecy."[132]

The court rejected Copenhefer's argument, stating that Copenhefer merely had a hope of privacy when he deleted the files and because the files were still in the computer's memory they could be recovered by any means that the government could employ.[133] In essence, the court is stating that merely hoping that something remains secret is not enough to create a reasonable expectation of privacy. When a file is deleted, a computer does not really dispose of it, but merely pushes it to the side and makes it available to be used if needed.[134] When file space is needed, these pushed-aside files are overwritten and become no longer recoverable.[135] When Copenhefer deleted his files they were not actually destroyed; they were just moved. Accordingly, there was no reasonable expectation of privacy in files merely believed to be secret because there was no actual protection—the files were still there.[136]

Copenhefer does not translate to a proposition that encryption is similar to failing to permanently remove files from one's computer, which would render no Fourth Amendment protection. Orin Kerr offers this case to argue how courts will rule on encrypted documents.[137] In addition to Kerr's

---

130. *Id.* at 1355.

131. *Id.* at 1354.

132. *Id.* at 1356.

133. *Id.* "A mere hope for secrecy is not a legally protected expectation . . . . At best, [Defendant] had the hope of achieving secrecy, but his hope did not prohibit the state from subjecting validly seized physical evidence from any scientific analysis possible within current technology." *Id.*

134. Jim Williams, *Deleted Files Still There, at* http://netsecurity.about.com/library/weekly/aa070300a.htm and on file with author (last visited Sept. 1, 2002).

135. *Id.* The article notes that it is fairly easy to recover deleted documents:

> With the right software, it is relatively easy to recover deleted files from your hard drive. Some file recovery software can even work over a network connection. What this means is that if you have confidential information or documents on your computer, simply deleting them does not get rid of them and an enterprising person could, if he or she wanted to, get at those files on your hard drive and see your confidential information.

Id.

136. *Copenhefer*, 587 A.2d at 1356. The court notes that "[a]ppellant's *unsuccessful attempt* to delete documents or files from his computer did not create a legally protected expectation of privacy which would have required a second warrant before the prosecution applied technology to elicit the content of files buried in the memory of the computer." *Id.* (emphasis added).

137. *See* Kerr, *supra* note 9, at 513, 516-17. Kerr also extends this case further by arguing:

> The same would be true of a diary recorded in a private code. If we accepted appellant's argument, after seizing the diary pursuant to a valid search warrant, the state would be obligated to obtain a second warrant before it could attempt to read the diary by deciphering the code. Yet the diarist's obvious attempt to achieve secrecy does not create

argument, it could be argued that deleting a file is just like encrypting a file, which is an attempt to make the file unreadable by others. If this were the case, *Copenhefer* would lay the foundation for no Fourth Amendment protection in encrypted documents. However, encryption is different than merely hitting the delete key.

As stated in the encryption section of this article, encryption does not create just a mere hope that the document will remain secret; it virtually locks the document so no one but the user can read its contents.[138] This is the purpose of the encryption. So while it can be argued that deleting a document achieves the same effect, this is not actually the case.[139] Deleting a document does not fully erase or secure the document so that no one else will read it. Deletion is just a "mere hope for secrecy."[140] Encryption, in contrast, actually creates privacy in a document by not allowing anyone else to read it.[141]

In addition to pointing out the flawed reasoning in applying the above three cases to digital encryption, there seems to be cases that support the proposition that encryption creates a reasonable expectation of privacy.

D. Cases That Support the Protection of Encrypted Documents

In *Texas v. Brown*, police made a plain view seizure of a balloon filled with narcotics at an investigatory stop.[142] The Court found the search of the car to be valid under the plain view doctrine.[143] However, in his concurring opinion, Justice Stevens argued that the plain view doctrine justified the

---

> a legally protected expectation of privacy nor the need to obtain a warrant before subjecting legally seized physical evidence to scientific testing and analysis to make it divulge its secrets.

Id. at 517.

138. *See supra* notes 12-31 and accompanying text.

139. *See id.*

140. *Copenhefer*, 587 A.2d at 1356.

141. It has been argued that Copenhefer would have been helped by encryption in this case because deleting made a file still recoverable by the government. A. Michael Froomkin, *The Metaphor is the Key: Cryptography, The Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 729 n.62 (1995). This is the argument presented here: while deleting the file is merely a hope for privacy because it does not actually get rid of a file, encryption actually protects documents by getting rid of the possibility of someone else seeing them.

142. Texas v. Brown, 460 U.S. 730, 733-34 (1983).

143. *Id.* at 744. The Court noted, however, that "[o]ur cases hold that procedure by way of warrant is preferred." *Id.* at 735.

seizure of the party balloon, but additional justification was required to open the balloon without a warrant.[144]

The concurrence can be analogized to a situation where the government legally seizes information, but where there is still a reasonable expectation of privacy in the objects found. In this situation, a warrant would be needed to search further. Analogously, encryption could be treated as the balloon in *Brown* because it covers the document and creates a privacy interest. Reasoning with Justice Stevens, encryption would create a reasonable expectation of privacy.

While case law tends to demonstrate courts' trend toward granting encryption Fourth Amendment protection, or at least demonstrating that courts have not yet excluded encryption from protection, it could be argued that in situations where police seize a computer filled with encrypted documents, there is no need for another search warrant to decrypt the files. This argument would be based on the premise that the government should lawfully be able to do whatever it takes to get at these documents if they are legally using a computer or have legally seized the hard drive. However, courts have responded to this argument in other situations. *United States v. Turk*[145] shows that there can be an additional reasonable expectation of privacy in items lawfully searched. Reasoning under *Turk*, if encryption is afforded Fourth Amendment protection, then encrypted files would have *additional* protection if the government had legally seized the object that contained these digital documents.

This type of additional protection is seen in *United States v. Block*.[146] In *Block*, the defendant was living with his mother.[147] The defendant's mother had free access to the defendant's room and used that access to consent to a search of his room by the government.[148] However, while her consent to search the room was valid, the court held that she did not have the authority

---

144. *Id.* at 750 (Stevens, J., concurring). It is significant to note Justice Stevens's reasoning in this case:

> [I]f there is probable cause to believe it contains contraband, the owner's possessory interest in the container must yield to society's interest in making sure that the contraband does not vanish during the time it would take to obtain a warrant. The item may be seized temporarily. It does not follow, however, that the container may be opened on the spot. Once the container is in custody, there is no risk that evidence will be destroyed. Some inconvenience to the officer is entailed by requiring him to obtain a warrant before opening the container, but that alone does not excuse the duty to go before a neutral magistrate.

Id. at 749-50.

145. 526 F.2d 654 (5th Cir. 1976) (holding that although the seizure of a tape was proper, playing the taped conversation of private telephone communication was not because there was a reasonable expectation of privacy in the tape).

146. 590 F.2d 535 (4th Cir. 1978).

147. *Id.* at 537.

148. *Id.* at 541.

to consent to the search of a footlocker that was located in the room.[149] The footlocker was afforded additional protection because it was a particular object with an additional expectation of privacy.[150] This situation is similar to situations where the government has lawful access to a computer that they are searching.

The abovementioned situation was addressed in *Trulock v. Freeh*.[151] In *Trulock*, the defendant's townhouse and computer were searched after the defendant's roommate, who had access to all areas of the townhouse and Defendant's computer, consented to a search of Defendant's property.[152] Among the things searched were the defendant's password protected documents located in her computer's hard drive.[153] The court held that the search of the computer was valid.[154] However, the court found that the search of the password-protected files was invalid because the files carried an additional expectation of privacy.[155] The court wrote: "[a]lthough [Defendant's roommate] had authority to consent to a general search of the computer, her authority did not extend to Trulock's password-protected files."[156] They reasoned that because the defendant concealed his password and protected the files that he had a reasonable expectation of privacy.[157] While the court refused to recognize a clearly established right in regard to password protected files[158], this decision shows that the trend of at least one court is to afford password protected documents a reasonable expectation of privacy.

VI. ENCRYPTION TECHNOLOGIES SERVE AS THE LOCKS AND KEYS OF CYBERSPACE

The lock-and-key metaphor, relating encryption to a physically locked container, may be the lynchpin of unrolling the Fourth Amendment's protective cover over encrypted documents.[159] If encryption is found to be

149. *Id.*
150. *Id.*
151. 275 F.3d 391 (4th Cir. 2001).
152. *Id.* at 398.
153. *Id.*
154. *Id.* at 403.
155. *Id.*
156. *Id.*
157. *Id.*
158. *Id.*
159. *See* Froomkin, *supra* note 141; Michael Adler, *Cyberspace, General Searches and Digital Contraband: The Fourth Amendment and the Net-Wide Search*, 105 YALE L.J. 1093 (1996); Lennon,

the cyber equivalent of physical locks and keys, then the Court will most likely give the same Fourth Amendment protection to encryption that it has given to certain physical containers that seal possessions.[160] The Court wrote that "[a] container which can support a reasonable expectation of privacy may not be searched, even on probable cause, without a warrant."[161] Locking something is an effective expression of a person's reasonable expectation of privacy.[162] Consequently, a warrant is needed to open a locked box[163] and, reasoning that encryption is similar, a warrant would have to be obtained to "open" an encrypted document.[164]

Orin Kerr argues that encryption does not work like a physical lock that closes off objects from the eye.[165] Encryption, according to Kerr, works by making something unrecognizable and thus does not work like a lock.[166] This argument is modernly lacking in that it does not correctly apply the analogy to the digital world, where users expect encryption to act as a lock.[167] The physical lockbox usually hides its contents with solid walls. This makes *the contents* invisible by outsiders (which is typically the reason someone would put something in the box). Encryption acts in the same way.

---

supra note 61, at 467.

160. United States v. Jacobsen, 466 U.S. 109, 120, n.17 (1984).

161. *Id.*

162. Walter v. United States, 447 U.S. 649, 658 (1980) (illustrating that wrapping or locking an object manifests a reasonable expectation of privacy).

163. United States v. Presler, 610 F.2d 1206, 1213-14 (4th Cir. 1979) (holding that the act of locking a briefcase and then retaining the only means of access to it – a key or combination – is an effective manifestation of an expectation of privacy). *See also*, United States v. Barry, 853 F.2d 1479, 1482 (8th Cir. 1988) (finding a reasonable expectation of privacy in a locked suitcase left at the Minneapolis-St. Paul Airport); United States v. Benson, 631 F.2d 1336, 1338-39 (8th Cir. 1980) (finding a reasonable expectation of privacy in a closed but unlocked leather tote bag).

164. Froomkin, *supra* note 141.

165. Kerr, *supra* note 9, at 520, 522-24.

166. *Id.* at 520-24. Kerr believes "[t]he trick to understanding why the Fourth Amendment distinguishes between a physical lock-and-key and the lock of encryption is to realize that the two cases rely on two very different meanings of the word 'lock.'" *Id.* at 521. He distinguishes the two by noting that a physical lock and key "limits the movement of two or more surfaces relative to each other" while encryption locks a document by making the "communication inaccessible by making it incomprehensible." *Id.* Kerr believes that encryption "locks" something by making it complex and unintelligible to most. *Id.*

167. It is important to remember that the Court determines what someone reasonably expects when they want privacy in addition to looking at whether society will accept the expectation as reasonable. *See supra* notes 39-87 and accompanying text. Patrick Brethour, *Hacker Hits Microsoft Software Web Music Anti-Piracy Program Outfoxed*, GLOBE & MAIL, Oct. 23, 2001, at B4 (noting that users employ "encryption technology to lock down content in whatever manner the author specifies"); Shannon Tan, *Program May Allow Hackers to Gain Data from Internet in Miami Area*, MIAMI HERALD, Aug 28, 2001; (noting individuals that use encryption to lock documents); John Fontana, *Public Key Infrastructure May Provide True E-Commerce Security*, COLORADO BUS., July 1, 2001 ("A set of encryption keys that work in concert to lock and unlock information as part of secure PKI transactions."). *See generally* Crain, *supra* note 4, at 870 (stating that "Encryption technologies serve as the locks and keys of cyberspace.").

Encryption makes a document invisible to outsiders that do not have the key. Instead of using physical walls, it creates a digital wall by constructing a set of symbols that mean nothing without the encryption key.[168] Encryption does not merely make a document "incomprehensible" or "hard to understand;"[169] encryption makes a document impossible to view, which effectively creates a digital wall.[170]

The fact that encryption achieves this digital wall through encoding, creating an "incomprehensible" language, is inconsequential to the analogy. The incomprehensible symbols that an encryption engine creates are the very basic particles to the encryption. In cyberspace these symbols would be equivalent to the atoms that compose the physical world. It would be ridiculous to argue in the physical world that since we could decode the atomic code and see through the locked box utilizing an x-ray that there should be no Fourth Amendment protection to this atomically "incomprehensible" locked box. The same analogy seems foolish in cyberspace.

VII. CONCLUSION

If this issue is ever presented to the Supreme Court, the Court should hold that encryption creates a reasonable expectation of privacy and is thus protected under the Fourth Amendment. The process of encryption provides more security and protection than most things in the physical world. It seems logical to afford privacy protection to something that secures data so well that a supercomputer would have to work thousands of years to break the protection. The framers of the Constitution used encryption to protect their documents. With this, it is argued that they had encryption in mind when they were proposing the right to privacy. The evolution of the right to privacy demonstrates that the Court seems to want to cover encryption under Fourth Amendment protection. It also seems that current courts are starting to move toward affording electronic communications, especially ones that have been encrypted, Fourth Amendment protection. It becomes apparent

168. *See supra* notes 12-31 and accompanying text.

169. *See* Kerr, *supra* note 9, at 521.

170. *Id.* This is meant to refute Kerr's argument that encryption just makes something hard to understand, but not impossible to understand. However, it does create the question: how incomprehensible is incomprehensible enough for the Fourth Amendment? From previous case law it would appear that completely sealed objects create a reasonable expectation of privacy. Does encryption create a completely sealed object? From the perspective of the layperson encryption is unbreakable. From the perspective of a supercomputer, it could take up to 1000 years (or be impossible altogether) to pick the cyber-lock.

that encryption will be protected when described in terms of the lock-and-key analogy. With all of this, it seems that encryption is not only a method that can be used reasonably to expect to keep data private, but also a method that is constitutionally protected.

Sean J. Edgett

Pepperdine University School of Law