KEEPING SECRETS: A CONSTITUTIONAL EXAMINATION OF ENCRYPTION REGULATION IN THE UNITED STATES AND INDIA

Scott Brady*

I. INTRODUCTION

In July 2010 the Indian Ministry of Telecommunications revived a standing threat to ban BlackBerry services within the country.[1] Concerned that the BlackBerry messaging system could serve as a method of communication for dissidents, the Ministry demanded that mobile phone developer Research in Motion (RIM) provide government officials with access to encrypted corporate emails.[2] India's Ministry of Home Affairs and the Department of Telecommunications threatened, "If they don't follow our guidelines, we will have no option but to ask them to stop their operations in India."[3] "[RIM has] so far denied data on the excuse of encryption."[4]

The July threat was predicated upon a series of terrorist attacks that occurred in India two years prior.[5] In 2008 Lashkar-e-Taiba, a Pakistan-based militant organization, executed violent terror attacks in Mumbai, India, leaving at least 173 people dead and hundreds more wounded.[6] "Mobile phones, including BlackBerry smartphones . . . were used to coordinate the assault."[7] The horrific Mumbai attacks confirmed apprehensions expressed by India's security services more than a year before the assault.[8] Indian officials had long been lobbying against the BlackBerry smartphone, claiming "that criminals, militants, and terrorists could use BlackBerrys to send encrypted messages[, which government] agencies could neither intercept, trace, nor decode."[9] The

---

* J.D., 2012, Indiana University Robert H. McKinney School of Law.

1. Sahil Makkar & Shauvik Ghosh, *India Renews Threat to Ban BlackBerry Services*, WALL ST. J. (as partner) (July 29, 2010), http://www.livemint.com/2010/07/28200607/India-renews-threat-to-ban-Bla.html.

2. Yousif Abdullah, *RIM and the Middle East – An Analysis*, CRACKBERRY.COM (Sept. 22, 2010), http://crackberry.com/rim-and-middle-east-analysis; Tim Conneally, *RIM: No Back Door into Encrypted BlackBerry Messages for Any Government*, WORLDTECH24 (Aug. 3, 2010), http://www.worldtech24.com/business/rim-no-back-door-encrypted-blackberry-messages-any-government.

3. Conneally, *supra* note 2.

4. Makkar & Ghosh, *supra* note 1.

5. Abdullah, *supra* note 2.

6. *Id.*

7. *Id.*

8. ALASTAIR SWEENY, BLACKBERRY PLANET: THE STORY OF RESEARCH IN MOTION AND THE LITTLE DEVICE THAT TOOK THE WORLD BY STORM 195 (2009).

9. *Id.* at 195-96.

Indian government proposed to require that RIM install servers in India so that the nation's security services could monitor and intercept smartphone traffic.[10]

The problem: data encryption. Indian intelligence agencies are unable to decipher encrypted data sent across BlackBerry corporate servers.[11] The BlackBerry security architecture is based on a symmetric system of encryption, whereby the customer creates an individualized access key, enabling only that user to decode messages received.[12] Although the government can legally intercept smartphone communications, because the information received is coded, government agents are unable to convert these messages into a readable plaintext without RIM's cooperation.[13]

India's threat to ban encrypted BlackBerry communications evokes a re-examination of the long-standing debate surrounding the constitutionality of encryption, a debate that pervades many nations.[14] In the United States, the constitutionality of encryption has been examined for more than twenty years.[15] In both India and the United States, government requests to compel the production of an encryption key trigger the constitutional protections of privacy and due process.[16] However, the composition and interpretation of the U.S. and Indian Constitutions differ, yielding slightly different results.[17] Although both nations have sought to compel decryption, their approaches, and ultimately their outcomes, reflect this difference.[18]

This Note offers a comparative examination of the U.S. and Indian approaches to compel decryption from a constitutional perspective. It is presented in six parts. Part II provides a brief explanation and history of cryptography, including an introduction to modern data encryption technology. Part III presents the U.S. approach to compel decryption. This Part examines constitutional encryption protection under the Fourth and Fifth Amendments and the contemporary government attempts at decryption compulsion. Part IV explores the parallel approach to compel decryption in India, examining constitutional encryption protection under Article 21 and contemporary government attempts to compel decryption. Within this comparative analysis, this Note reveals important distinctions between the U.S. and Indian Constitutions with respect to the protection of fundamental human rights. Part V presents recommendations for striking a balance between civil liberties and

10. *Id.* at 196.

11. Makkar & Ghosh, *supra* note 1.

12. Conneally, *supra* note 2.

13. Joel C. Mandelman, *Lest We Walk into the Well: Guarding the Keys – Encrypting the Constitution: To Speak, Search & Seize in Cyberspace*, 8 ALB. L.J. SCI. & TECH. 227, 272 (1998).

14. *See infra* Parts III-V.

15. *See infra* Part III.E.2.

16. *See infra* Parts III, IV.

17. *See id.*

18. *See id.*

national security. The sixth part concludes this Note.

II. HISTORY OF CRYPTOGRAPHY

A. Early Encryption

Cryptography, the science of writing in secret code, enables a person to safeguard sensitive information by preventing unauthorized access to the content of a message.[19] Society has employed cryptography to protect important correspondence throughout history.[20] One of the earliest reported examples of the practice involved tattooing a message on the scalp of a slave.[21] Once the slave's hair grew back, the slave would be sent to the message's recipient, who would re-shave the slave's head, thus revealing the secret communication.[22]

Early American colonists employed cryptography at the onset of the country's independence.[23] Because the British government frequently opened the colonists' private mail, and because mail was easily stolen, "there was a substantial risk of exposure in colonial America."[24] As a result, the young nation's leaders used codes and ciphers to preserve the confidentiality of their communications.[25] Given its historical context, it has been argued that the privilege of encryption is an "ancient liberty": "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."[26]

B. Modern Encryption Technology

Although primitive forms of encryption have existed for thousands of years, modern technological advances have transformed encryption into a complex process.[27] Similar to its rudimentary methods, modern-day encryption still involves the transformation of plaintext communication into ciphered text

---

19. Brendan M. Palfreyman, Note, *Lessons from the British and American Approaches to Compelled Decryption*, 75 BROOK. L. REV. 345, 348 (2009).

20. *Id.* at 349.

21. *Id.*

22. *Id.*

23. 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, para 20 (1997).

24. *Id.*

25. *Id.* paras. 21-40.

26. *Id.* para 2. Fraser offers an extensive examination of encryption throughout American history, including colonial, revolutionary, constitutional, nineteenth century, twentieth century, and modern day encryption. *See generally id.*

27. Palfreyman, *supra* note 19, at 350.

messages.[28] However, the contemporary encryption process uses sophisticated digital algorithms to cipher the communications.[29] This process creates a highly secured encrypted text, which is readable only by a recipient possessing the proper key.[30]

Present-day digital encryption requires the employment of an "encryption key."[31] In its simplest terms, an encryption key is a digital code that corresponds with an encryption cipher to "unlock" a message, converting the communication into readable plaintext.[32] These keys usually consist of long strings of numbers stored within a personal electronic device.[33] Typically, the recipient of a message does not need to memorize this code but may enter a simple password, created by the user, to access the embedded encryption key.[34]

There are two primary encryption key systems: private key and public key.[35] A private key encryption involves the employment of only one key, which is used for both encrypting and decrypting a coded message.[36] In this system, the sender uses a private key to encrypt a message, and the receiver uses that same private key to decode the message.[37] In contrast, public key encryption (also referred to as asymmetric encryption) employs two keys, a public key for encryption and a private key for decryption.[38] In this system, the public encryption code is available for all users, but the private key is unique to the receiver.[39] Although messages may be easily encrypted with the public key, private key access is essential for decryption.[40] Today, public key encryption is the most common system of digital encryption.[41] Private key access is the strength of this system, as it is "computationally infeasible" to acquire a private key from the public key.[42] "[I]t is virtually impossible to break strong public key encryption without compelling, or otherwise obtaining, direct access to the private key."[43]

---

28. *See* Ashwin Satyanarayana, *Fundamentals of Network Security: Understanding Encryption and Decryption*, BRIGHT HUB (Sept. 17, 2009), http://www.brighthub.com/computing/enterprise-security/articles/7732.aspx (last updated July 14, 2011).

29. *See id.*; *Cryptography*, THEFREEDICTIONARY.COM, http://encyclopedia2.thefreedictionary.com/Cryptography (last visited May 14, 2012).

30. *See* Satyanarayana, *supra* note 28; *Crytography*, *supra* note 29.

31. *Cryptography*, *supra* note 29.

32. *Id.*

33. *Id.*

34. Conneally, *supra* note 2.

35. Palfreyman, *supra* note 19, at 351.

36. *Id.*

37. *Id.*

38. *Id.*

39. *Id.*

40. *Id.*

41. *Id.* at 350.

42. Palfreyman, *supra* note 19, at 351.

43. *Id.* at 352.

III. THE UNITED STATES APPROACH

The modern constitutions of the United States and India were "constructed and forged in two very distinct and unique political and cultural settings."[44] They have in common, however, one important context: each country chartered its Constitution after gaining independence from the British Raj.[45] The Supreme Courts of these former British colonies have developed "doctrines of due process and jurisprudential traditions of activism that [have] expanded the scope [and understanding] of fundamental rights."[46]

A. Constitutional Foundation

The U.S. Constitution is "animated by and premised on" a desire to limit the strength of the federal government through the separation of powers.[47] Before drafting the Constitution, the young nation was "held together by the tenuous threads of the Articles of Confederation."[48] Desiring a divergence from this confederate structure, the Constitutional Assembly advocated the necessity of both horizontal and vertical separation of powers.[49] Exemplifying this ideal, James Madison declared:

> [B]y so contriving the interior structure of the government as that its several constituent parts may, by their mutual relations, be the means of keeping each other in their proper places . . . . But what is government itself, but the greatest of all reflections on human nature? If men were angels, no government would be necessary.[50]

---

44. Manoj Mate, *The Origins of Due Process in India: The Role of Borrowing in Personal Liberty and Preventive Detention Cases*, 28 BERKELEY J. INT'L L. 216, 216 (2010).

45. *Id.*

46. *Id.* at 216-17.

47. *Id.* at 224.

48. *Constitutional Topic: The Constitutional Convention*, USCONSTITUTION.NET, http://www.usconstitution.net/consttop_ccon.html (last visited Mar. 23, 2012) [hereinafter *The Constitutional Convention*]. Drafted in 1777 by the Continental Congress, the Articles of Confederation served as the first constitution of the United States. *The Articles of Confederation*, USCONSTITUTION.NET, http://www.usconstitution.net/articles.html (last visited Mar. 23, 2012). The Articles established a "firm league of friendship" between and among the thirteen American States. *Id.* Created during the turmoil of the Revolutionary War, the Articles reflected a distrust of strong central government: a philosophy that remained steadfast throughout the drafting of the Constitution. *See id.* Although the Articles effectuated a united nation, the Articles denied Congress the power to collect taxes, regulate interstate commerce, and enforce laws. *Id.* These shortcomings eventually led to the adoption of the Constitution. *See id.*; *see also* ARTICLES OF CONFEDERATION, in 19 JCC 214 (Mar. 1, 1781).

49. *See* Mate, *supra* note 44, at 224.

50. THE FEDERALIST NO. 51, at 314 (James Madison) (Clinton Rossiter ed., 1961).

In addition to the composition of a separated, limited government, the U.S. Constitution is saturated with provisions protecting the value of privacy.[51] Preceding its interpretation into the U.S. Constitution, the right of privacy was fundamental in the minds and hearts of Americans.[52] American colonists "believed a man's home was his castle," to which any without entry invitation constituted a trespass.[53] When drafting the Bill of Rights, the Constitutional Assembly discussed which fundamental values to preserve within the Constitution.[54] Of these, "[p]rivacy was a central concern."[55] In American minds, the right to privacy is a "right most valued by civilized people [sic]."[56]

B. Fourth Amendment Analysis

An examination of encryption under the U.S. Constitution begins with the Fourth Amendment. The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[57]

This Amendment initially served to protect the privacy of an individual's home or business and everything that occurred within its walls.[58] However, as technology has advanced, Fourth Amendment jurisprudence has evolved to encompass new privacy issues.[59]

The Supreme Court has expanded the scope of individual privacy rights to include constitutionally protected electronic communications.[60] Assurance against the government's unlawful seizure of an individual's encryption key

---

51. *See generally* Griswold v. Connecticut, 381 U.S. 479 (1965) (holding that penumbras from other constitutional rights establish the right to privacy, which is protected by the Constitution).

52. Hillary Victor, Comment, *Big Brother Is at Your Back Door: An Examination of the Effect of Encryption Regulation on Privacy and Crime*, 18 J. MARSHALL J. COMPUTER & INFO. L. 825, 835-36 (2000).

53. *Id.* at 836.

54. *Id.*

55. *Id.*

56. Nan Hunter et al., *Contemporary Challenges to Privacy Rights*, 43 N.Y.L. SCH. L. REV. 195, 197 (1999) (quoting Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting)).

57. U.S. CONST. amend. IV.

58. Victor, *supra* note 52, at 836.

59. *Id.* at 836-37.

60. *Id.* at 837.

arguably is granted by these Fourth Amendment protections.[61] The foundation for this premise was developed through a series of Supreme Court cases examining the legality of non-physical invasions of privacy.[62] The first of these, *Olmstead v. United States*, began the constitutional debate of wiretapping in the United States.[63]

1. Olmstead v. United States

In *Olmstead v. United States*, the leading conspirator of an alcohol bootlegging campaign, Roy Olmstead, was the subject of government surveillance.[64] Federal prohibition officers discovered the conspiracy primarily through the interception of Olmstead's telephone conversations.[65] To accomplish this, small wires were inserted along the telephone lines of the conspirators' homes and those leading from Olmstead's chief office.[66] Olmstead was convicted notwithstanding his argument that the unwarranted wiretap search violated his Fourth Amendment rights.[67]

In a narrow decision, the Supreme Court held that the federal government had the authority to wiretap without a warrant under the Fourth Amendment because no physical intrusion occurred.[68] However, in a dissenting opinion, Justice Brandeis argued that wiretaps, even without physical invasion, were subject to Fourth Amendment protections.[69] Brandeis proclaimed,

> The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.[70]

Brandeis's dissent foreshadowed the conclusion of the Court's later decision in *Katz v. United States*, and typifies the contemporary argument for encryption protection under the Fourth Amendment.[71]

---

61. *Id.*
62. *See infra* Part III.B.1-4.
63. Olmstead v. United States, 277 U.S. 438 (1928).
64. *Id.* at 456.
65. *Id.*
66. *Id.* at 456-57.
67. *Id.* at 455.
68. *Id.* at 465-66.
69. *Id.* at 474.
70. *Id.*
71. *See* Katz v. United States, 389 U.S. 347, 353 (1967).

2. Katz v. United States

In *Katz v. United States*, a majority of the Supreme Court embraced Justice Brandeis's *Olmstead* dissent and specifically recognized the concept of privacy as implicit in the Fourth Amendment.[72] Charles Katz was charged with transmitting gambling wagers by telephone across state lines, in violation of federal law.[73] Incriminating evidence was obtained when Federal Bureau of Investigation (FBI) agents "attached an electronic listening and recording device to the outside of the public telephone booth from which . . . [Katz] placed his calls."[74] Ultimately, the Court held that the government's activities constituted a search and seizure within the meaning of the Fourth Amendment because the recording of conversations transmitted from the phone booth violated the privacy upon which Katz justifiably relied.[75] In a concurring opinion, Justice Harlan set forth a "reasonable expectation of privacy" test that was later adopted by the Supreme Court in *Terry v. Ohio*.[76]

The *Katz* decision has subsequently been codified and superseded by various federal and state laws. For example, concluding that the *Katz* standard was vague and inadequate,[77] Congress enacted legislation that added substantial requirements to the minimal constitutional protection outlined in *Katz*.[78] In contrast, the New York State Congress codified the standards crafted by the Supreme Court.[79] In compliance with the Fourth Amendment mandates outlined in *Katz*, the New York statute "contains detailed requirements regulating every aspect of wiretapping, as well as a procedure to suppress evidence when those requirements are not met."[80]

3. Contemporary Cases

To date, no cases have specifically resolved the issue of unwarranted encryption key production under a Fourth Amendment analysis. One federal district court, however, recently examined the constitutional validity of an unwarranted government seizure of cell phone data retrieved from a third party cell-site.[81] In *United States v. Benford*, the United States District for the Northern District of Indiana decided that the government's acquisition of a

72. *Id.*
73. *Id.* at 348.
74. *Id.*
75. *Id.* at 353.
76. *Id.* at 360-61; *see* Terry v. Ohio, 392 U.S. 1, 9 (1968).
77. United States v. Koyomejian, 946 F.2d 1450, 1455 (9th Cir. 1991).
78. *Id.*; *see* Communications Assistance for Law Enforcement Act, 18 U.S.C. §§ 2510-22.
79. N.Y. C.P.L. LAW § 700 (2010); *see* People v. Darling, 742 N.E.2d 596, 599 (N.Y. 2000).
80. *Darling*, 742 N.E.2d at 599.
81. United States v. Benford, 2010 U.S. Dist. LEXIS 29453, at *5 (N.D. Ind. 2010).

defendant's cell-site data does not violate the Fourth Amendment.[82] The court concluded that a person has no legitimate expectation of privacy in a third-party cell phone company's records identifying which cell phone towers communicated with that individual's cell phone.[83]

4. Criticism

The extension of constitutional protection to encryption, specifically the protection against unlawful search and seizure under the Fourth Amendment, is not without opposition. Some legal scholars argue that the debate is misplaced. Joel Mandelman, Vice President and General Counsel of Nutech H20, claims that the mandatory escrowing of encryption code keys from a Trusted Third Party (TTP) does not amount to a warrantless search and seizure,[84] as escrowing a TTP produces nothing of meaningful value.[85] The encryption key has no communicative or incriminating content of its own but is merely a tool for deciphering the intercepted communication.[86] In fact, more of a search and seizure occurs when the government intercepts the suspect's communication.[87] As long as the communication was intercepted pursuant to a warrant or subpoena, the encryption key will not be used to search anything but only to decipher that which the government lawfully has in its possession.[88] Articulating a "time is of the essence" policy argument for obtaining encryption keys, Mandelman believes it "wholly unrealistic to suggest that the government could get a warrant to seize the code key after the fact."[89]

C. Fifth Amendment Analysis

In addition to protection against unlawful search and seizure, compelled encryption production also invokes the privilege against self-incrimination guaranteed by the Fifth Amendment to the U.S. Constitution. The Fifth Amendment provides in part: "No person . . . shall be compelled in any criminal case to be a witness against himself."[90] This right, however, is not absolute. In order to trigger Fifth Amendment protection, three requirements must be met: (1) the disclosure must be testimonial, (2) the disclosure must be

82. *Id.* at *8 (adopting the logic expressed by the Supreme Court in Smith v. Maryland, 422 U.S. 735 (1979), and United States v. Miller, 425 U.S. 435 (1976)).

83. *Id.*

84. Mandelman, *supra* note 13, at 268.

85. *Id.* at 273.

86. *Id.* at 272-73.

87. *Id.* at 272.

88. *Id.* at 272-73.

89. *Id.* at 273.

90. U.S. CONST. amend. V.

compelled, and (3) criminal liability must be a possible result.[91] In certain circumstances, a government request to compel the production of an encryption key could satisfy these requirements, and the Fifth Amendment right against self-incrimination will be triggered.[92]

The first case to address compelled decryption under the Fifth Amendment was *In re Boucher (Boucher I)*.[93] In fact, "[t]his case forms the basis of the [U.S.] approach to compelled decryption under Fifth Amendment jurisprudence."[94] Sebastien Boucher was arrested during a U.S. customs inspection at the Canadian border for knowingly transporting child pornography.[95] The government seized a laptop computer from Boucher's vehicle, but the contents of the computer were password-protected and the government's forensics expert could not gain access.[96] Boucher was subpoenaed to surrender the password, but he refused to comply.[97] Boucher instead moved to quash the subpoena, arguing that the production of his password would violate his Fifth Amendment right against self-incrimination.[98]

In *Boucher I*, the United States District Court for the District of Vermont concluded that the production of a password has communicative aspects and is considered "testimonial" under the Fifth Amendment.[99] Citing *United States v. Doe*, the court reiterated, "'Although the contents of a document may not be privileged, the act of producing the document may be.'[100] By entering the password[,] Boucher would be disclosing the fact that he knows the password and has control over the files . . . ."[101] Thus, the court held that the surrender of an encryption password violated the Fifth Amendment privilege against self-incrimination, and Boucher's motion to quash the subpoena was granted.[102]

The decision in *Boucher I* was subsequently reversed in *In re Boucher (Boucher II)* by an application of the "foregone conclusion doctrine."[103] Under this doctrine, if "the government is already aware of the existence and location of a particular document or file, and if producing the document or file would not 'implicitly authenticate' it, then any evidence gained would be a foregone

91. Palfreyman, *supra* note 19, at 353 (citing Fisher v. United States, 425 U.S. 391, 408 (1976)) ("Fifth Amendment . . . applies only when the accused is compelled to make a testimonial communication that is incriminating.").

92. *See id.* at 361.

93. In re Boucher (Boucher I), No. 2:06-mj-91, 2007 WL 4246473 (D. Vt. Nov. 29, 2007).

94. Palfreyman, *supra* note 19, at 353.

95. *Boucher I*, 2007 WL 4246473, at *2.

96. *Id.*

97. *Id.*

98. *Id.*

99. *Id.* at *3.

100. *Id.* (citing United States v. Doe, 465 U.S. 605, 612 (1984)).

101. *Id.*

102. *Id.* at *6.

103. In re Boucher (Boucher II), No. 2:06-mj-91, 2009 WL 424718, at *4 (D. Vt. Feb. 19, 2009).

conclusion, and the suspect would not be entitled to Fifth Amendment protection."[104] In reversing its original holding, the court determined that because government agents were able to view Boucher's files before they were encrypted, and because Boucher admitted that the computer was his, the foregone conclusion doctrine applied.[105] Thus, Boucher was directed to comply with the subpoena and surrender an unencrypted version of his computer drive.[106] Despite its technical reversal in *Boucher II*, the holding of *Boucher I* exemplifies the U.S. approach to encryption regulation under the Fifth Amendment: compelled password disclosure may have testimonial aspects, and the privilege against self-incrimination may be invoked to avoid involuntary compliance with a government request for surrender.[107]

D. Act-of-Production Doctrine

A constitutional analysis of encryption regulation also implicates the "act-of-production doctrine," a derivative of the Fifth Amendment privilege against self-incrimination.[108] "Judges have handled compelled data decryption under the umbrella of this doctrine largely because they have analogized an encrypted hard drive to a virtual wall safe from which the accused is asked to remove incriminating papers."[109]

1. Boyd v. United States

The act-of-production doctrine was first introduced in *Boyd v. United States*.[110] In *Boyd*, the government subpoenaed business invoices from E. A. Boyd & Sons (Boyd) during a smuggling investigation of the company.[111] Against Boyd's objections, the documents were later admitted at trial, which resulted in Boyd's conviction.[112] Reversing the lower court's order of production, the United States Supreme Court interpreted the Fifth Amendment broadly, holding that the compulsory production of private books and papers is tantamount to self-incrimination.[113] The Court stated, "[W]e have been unable to perceive that the seizure of a man's private books and papers to be used in evidence against him is substantially different from compelling him to be a

104. Palfreyman, *supra* note 19, at 360.
105. *Boucher II*, 2009 WL 424718, at *3-4.
106. *Id.* at *4.
107. Palfreyman, *supra* note 19, at 361.
108. Andrew J. Ungberg, Note, *Protecting Privacy Through a Responsible Decryption Policy*, 22 HARV. J. L. & TECH. 537, 542 (2009).
109. *Id.*
110. Boyd v. United States, 116 U.S. 616, 622 (1886).
111. *Id.* at 618.
112. *Id.*
113. *Id.* at 634-35.

witness against himself."[114]

2. Fisher v. United States

The *Boyd* decision guided the act-of-production doctrine well into the twentieth century. However, the Supreme Court eventually overruled it in *Fisher v. United States*, establishing the modern act-of-production doctrine.[115] In *Fisher*, the Internal Revenue Service had summoned the attorneys of Solomon Fisher and C.D. Kashmir, two clients accused of tax crimes, and directed them to produce their clients' tax documents.[116] Each attorney declined to comply with the production request, claiming that enforcement would compel self-incrimination in violation of the Fifth Amendment.[117]

The Court held "that the *Fifth Amendment* does not independently proscribe the compelled production of every sort of incriminating evidence but applies only when the accused is compelled to make a *testimonial* communication that is incriminating."[118] Because the clients' tax documents had been prepared voluntarily, the Court found that they could not be considered compelled testimony.[119] Although the Court foreclosed any claim to the privilege for voluntarily prepared documents, *Fisher* did not eliminate the privilege for an individual facing a subpoena *duces tecum*.[120] "The Court recognized that while the content of the incriminating documents was not privileged, the act of producing the documents itself might communicate facts."[121] It is under this facet of document production that the compelled decryption examination falls.

3. Contemporary Cases

The modern act-of-production doctrine has been critically developed through a variety of contemporary cases. With the *Fisher* decision as its foundation, the Supreme Court has often distinguished circumstances in which production may be non-testimonial, such as when the government has specific knowledge of the information contained in a document.[122] Where the government is fishing for information, however, the Fifth Amendment privilege

114. *Id.* at 633.

115. Ungberg, *supra* note 108, at 542; *see also* Fisher v. United States, 425 U.S. 391, 414 (1976).

116. *Fisher*, 425 U.S. at 394.

117. *Id.* at 395.

118. *Id.* at 408 (emphasis added).

119. *Id.* at 409-10.

120. Ungberg, *supra* note 108, at 543.

121. *Id.*

122. *Id.* at 544-45.

prevents production.[123]

E. Attempts to Compel Decryption

Prior to 1960 there is no evidence that the U.S. government wished to regulate the private use of encryption technology.[124] In 1977, in conjunction with the National Security Agency (NSA), the National Bureau of Standards certified an encryption chip known as the Data Encryption Standard (DES).[125] By 1987, however, the NSA developed a policy opposing private encryption research and development and decided it would no longer guarantee DES security.[126] Thereafter the U.S. government has continually attempted to compel decryption through executive and administrative action.[127]

1. The Clipper Chip

In the late 1980s, DES became "an international standard for cryptography."[128] By 1993 it was of such widespread use that the standard key was at risk of being compromised by intelligent interceptors.[129] This vulnerability provided the U.S. government with the "opportune moment to launch its campaign for the adoption of a new government-provided encryption product": the Clipper Chip (the "Clipper").[130]

Concerned that new communication technology would "frustrate lawful government electronic surveillance," the Executive Administration launched the Clipper campaign to protect national security interests.[131] President Clinton especially feared that sophisticated encryption technology would be used to "thwart foreign intelligence activities critical to our national interests."[132] Under the Clipper Chip proposal, the government sought to serve as its own escrow

123. *Id.* Ungberg discusses the development of the modern act of production doctrine through an examination of contemporary case law. *See generally id.*

124. Fraser, *supra* note 23, para. 50.

125. *Id.* para. 63.

126. *Id.*

127. The U.S. Congress has almost annually introduced an act that has, in some form, addressed encryption regulation. Often, the purpose of the proposed legislation is not directed at compelled decryption, but House Committees will attempt to earmark the bill with a provision to either reduce or improve the freedom of encryption. Much of the proposed legislation did not pass. This article does not have the capacity to highlight all related congressional activity, but aims to frame the current debate with the most significant legislative action.

128. Fraser, *supra* note 23, para. 64.

129. *Id.*

130. *Id.*

131. OFFICE OF THE PRESS SECRETARY, THE WHITE HOUSE, FACT SHEET: PUBLIC ENCRYPTION MANAGEMENT (Apr. 16, 1993), *available at* http://epic.org/crypto/clipper/white_house_factsheet.html.

132. *Id.*

agent for the encryption keys of all private citizens.[133] The Clipper thereby would enable the government to access all encrypted private communications.[134]

Upon its release and publication, the Clipper campaign was immediately criticized by the United States public.[135] On June 9, 1993, then-Director of Computer Professionals for Social Responsibility Marc Rotenberg best articulated these critical sentiments in his testimony against the Clipper before the House of Representatives.[136] Rotenberg argued that the Clipper Chip undermined the central purpose of the Computer Security Act and did not reflect public goals.[137] Moreover, he emphasized to Congress, "there is one point about the law that should be made very clear: currently there is no legal basis – in statute, the Constitution or anywhere else – that supports the premise which underlies the Clipper proposal."[138] Elaborating on his constitutional argument, Rotenberg claimed that "[t]he Fourth Amendment and the federal wiretap statute do not so much balance competing interests as they erect barriers against government excess and define the proper scope of criminal investigation."[139]

Echoing Rotenberg's opposition, congressional committees continued to attack the validity of the Clipper campaign for the next three years.[140] The Clipper proposal was initially postponed and eventually abandoned in 1996.[141] Finally, in 1998 Skipjack, the encryption algorithm developed for the Clipper Chip, was declassified.[142]

2. Comprehensive Counter-Terrorism Act of 1991

By the end of the 1980s, the United States had a strong standing federal law protecting electronic privacy, the Electronic Communications Privacy Act (ECPA).[143] However, this law had no particular effect on the analog transmission standard used by cellular communication technology at that

---

133. *Id.*

134. *The Clipper Chip*, EPIC, http://epic.org/crypto/clipper/ (last visited May 11, 2012).

135. *See id.*

136. *Encryption Technology and Policy, Hearing Before the S. Comm. on Telecomm. & Fin. and the Comm. on Energy & Commerce*, 103d Cong. (1993) (testimony and statement of Marc Rotenberg, Dir. CPSR Wash. Office), *available at* http://cpsr.org/prevsite/program/clipper/cpsr-markey-testimony-6-9.html/.

137. *Id.*

138. *Id.*

139. *Id.*

140. *See The Clipper Chip*, *supra* note 134.

141. Lawrence Wright, *The Spymaster*, NEW YORKER (Jan. 21, 2008), http://www.newyorker.com/reporting/2008/01/21/080121fa_fact_wright?printable=true.

142. *Skipjack Encryption*, TROPICAL SOFTWARE, http://www.tropsoft.com/strongenc/skipjack.htm (last visited Mar. 24, 2012).

143. *See* Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-22 (1986).

time.[144] Soon after the enactment of the ECPA, law enforcement officials began to express apprehension about the newly developed, more secure system of cellular encryption technology.[145] In particular, the FBI began a campaign "to see that robust electronic privacy protection systems [did not] become generally available to the public."[146]

Alarmed by the task of deciphering encrypted communications, in 1991 the FBI encouraged then-Senator Joe Biden[147] to introduce language in the proposed Comprehensive Counter-Terrorism Act (CCTA) that directed electronic service providers to allow government access to encrypted communications.[148] In January of that year, Senator Biden introduced the CCTA, including a subtitle addressing electronic communications, on the Senate floor.[149] The relevant provision on compelled decryption stated, "[P]roviders of electronic communications services and manufacturers of electronic communications service equipment shall ensure that communications systems permit the government to obtain the plain text contents of voice, data, and other communications when appropriately authorized by law."[150]

The CCTA provision raised widespread concern in the computer community, and by August 1991 the Electronic Frontier Foundation, in cooperation with Computer Professionals for Social Responsibility and other industry groups, successfully lobbied to have it removed from the bill.[151] The bill encountered further opposition associated with the encryption provision as well as other contested portions, failed to obtain the necessary congressional support, and was never adopted.[152]

Despite its rejection, the CCTA foreshadowed the FBI's anti-encryption legislation that followed.[153] Shortly thereafter, the FBI promoted the Violent Crime Control Act (VCCA) and the Communications Assistance for Law Enforcement Act (CALEA).[154] In the VCCA, once again through Senator

144. John Perry Barlow, *Decrypting the Puzzle Palace*, EFFECTOR ONLINE (July 29, 1992), http://w2.eff.org/effector/effect03.01.

145. *Id.*

146. *Id.*

147. In the 1990s Joe Biden served as the Senate Chairman of the Judiciary Committee. *Vice President Joe Biden*, WHITE HOUSE, http://www.whitehouse.gov/administration/vice-president-biden (last visited May 15, 2012). Joe Biden is the current Vice President for the Barack Obama Administration. *Id.*

148. *Id.*; *see* Comprehensive Counter-Terrorism Act of 1991, S. 266, 102d Cong. (1st Sess. 1991).

149. S. 266, § 2201.

150. *Id.* Biden introduced identical language in the Violent Crime Control Act of 1991. *See* Violent Crime Control Act of 1991, S. 618, § 545, 102d Cong. (1st Sess. 1991).

151. Barlow, *supra* note 144.

152. *Id.*

153. Declan McCullagh, *Joe Biden's pro-RIAA, pro-FBI Tech Voting Record*, CNET NEWS (Aug. 23, 2008), http://news.cnet.com/8301-13578_3-10024163-38.html?tag=mncol;txt.

154. *See* Violent Crime Control Act of 1991, S. 618, 102d Cong. (1st Sess. 1991); *and see* Communications Assistance for Law Enforcement Act, H.R. 4922, 103d Cong. (1994).

Biden's recommendations, the FBI made a second attempt to promote a statutory provision directing providers of electronic communications services to implement only such encryption methods as would assure governmental ability to extract from the data stream the plain text of any voice or data communications.[155] The language of the provision was identical to that proposed in the CCTA,[156] and like its predecessor, the bill faced immediate opposition and was not adopted into law.[157]

3. Communications Assistance for Law Enforcement Act of 1994

CALEA took a different approach than its predecessors; it attempted to restrict encryption without backdoors.[158] The purpose of the Act was "to make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes, and for other purposes."[159] The legislation sought to enable law enforcement to legally conduct electronic surveillance while protecting the right of privacy.[160] The law clarifies the statutory obligation of telecommunication service providers to assist law enforcement in the execution of electronic surveillance court orders.[161] CALEA requires that telecommunication service providers have the necessary technical capabilities to comply with surveillance requests;[162] specifically, carriers must be capable of "delivering intercepted communications and call-identifying information to the government, pursuant to a court order or other lawful authorization, in a format such that they may be transmitted by means of equipment, facilities, or services procured by the government."[163] Carriers must also facilitate the interception "unobtrusively and with minimum interference" to the subscriber's service.[164]

Although CALEA grants law enforcement broad authority to intercept communications and procure the necessary facilities to transmit information, the Act imposes limitations to protect reasonable expectations of privacy.[165] Of these limitations, the statute defines encryption as a specific exception to the

155. *See* S. 618, § 545.

156. *Compare id. with* Comprehensive Counter-Terrorism Act of 1991, S. 266, 102d Cong. § 2201 (1st Sess. 1991).

157. McCullagh, *supra* note 153.

158. *Id.*

159. Communications Assistance for Law Enforcement Act, P.L. 103-414, pmbl., 108 Stat. 4279 (1994).

160. ASK CALEA, http://www.askcalea.net/ (last updated June 22, 2011).

161. *Communications Assistance for Law Enforcement Act – CALEA*, GLOBALSECURITY.ORG, http://www.globalsecurity.org/intell/systems/calea.htm (last visited Mar. 24, 2012).

162. *Id.*

163. 47 U.S.C. § 1002(a)(3).

164. *Id.* § 1002(a)(4).

165. *Id.* § 1002(b).

rule.[166] CALEA provides, "A telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication."[167] Although the FBI conceded to the encryption exception, the bureau has sought ever since to discard the provision and has proposed the inclusion of mandatory encryption key recovery.[168]

Almost two decades after its enactment, CALEA has yet to be fully implemented.[169] The telecommunications industry has resisted the adoption of electronic surveillance capabilities as a basic element of its service through a series of litigation, extension requests, and other means.[170] In response, the Federal Communications Commission (FCC) "has undertaken a comprehensive review of issues relating to CALEA implementation . . . ."[171] The FBI has countered by continuing to monitor industry compliance efforts and seeking to expand the jurisdiction of the statute to include encryption regulation.[172] Although Congress made specific concessions for encryption in the 1994 bill, FBI officials argue that the mandatory imposition of encryption key recovery is comparable to CALEA's telecommunication requirements.[173] "[E]xperts have concluded that the FBI's demands for key recovery are not within the competence of the field, and would impose high degrees of risk of computer security."[174]

4. Pending Legislation

The U.S. government continues its attempt to compel decryption. The Obama administration is currently seeking the implementation of a new federal law that would compel encryption service providers to allow the government unrestricted surveillance access.[175] This law would compel communications providers to configure their systems such that law enforcement would be guaranteed access to deciphered information.[176] A supporter once again, the

166. *Id.* § 1002(b)(3).

167. *Id.*

168. *CALEA: A Precedent for Domestic Encryption Controls?*, CENTER FOR DEMOCRACY & TECH. http://www.cdt.org/digi_tele/cryptovscalea.html (last visited Feb. 4, 2011).

169. *See id.*; *see also Communications Assistance for Law Enforcement Act* – CALEA, *supra* note 161.

170. *Communications Assistance for Law Enforcement Act* – CALEA, *supra* note 161.

171. *Id.*

172. *CALEA: A Precedent for Domestic Encryption Controls*, *supra* note 168.

173. *Id.*

174. *Id.*

175. Declan McCullagh, *Report: Feds to Push for Net Encryption Backdoors*, CNET NEWS (Sept. 27, 2010), http://news.cnet.com/8301-31921_3-20017671-281.html [hereinafter *Net Encryption Backdoors*].

176. *Id.*

FBI contends that this legislation is "reasonable and necessary to prevent the erosion of their investigative powers."[177] With this proposal, the FBI stresses the importance of lawfully authorized interception of communications.[178] Valerie Caproni, general counsel for the bureau, stated, "We're not talking expanding authority. We're talking about preserving our ability to execute our existing authority in order to protect the public safety and national security."[179] This legislation represents the FBI's official attempt to extend CALEA's requirements to all digital communication providers and to dispose of the exception for encryption.[180]

When the administration's proposal is presented to Congress, it is expected to face a variety of obstacles, "including opposition from civil libertarian and business groups and concerns about its practicality and constitutionality."[181] Familiar critics are already expressing their concern with the reality of implementing a law of this nature.[182] Michael Sussmann, a former attorney for the Department of Justice (DOJ) commented, "It would be an enormous change for newly covered companies. Implementation would be a huge technology and security headache, and the investigative burden and costs will shift to providers."[183] Additionally, it has been argued that requiring service providers to permit interception would weaken the system and "inevitably be exploited by hackers."[184] Put simply by Steven Bellovin, a Columbia University computer science professor, "[I]t's a disaster waiting to happen."[185]

IV. THE INDIAN APPROACH

A. Constitutional Foundation

The Indian Constitution fundamentally differs from the U.S. Constitution in one significant manner—the Indian Constitution was authored considering the "'humanitarian socialist precepts[...]' at the heart '[...]of the Indian social revolution.'"[186] Unlike the limited government system created by the U.S. Constitution, the Indian Constitution establishes a strong government, modeled

177. Charlie Savage, *U.S. Tries to Make It Easier to Wiretap the Internet*, N.Y. TIMES (Sept. 27, 2010), http://www.nytimes.com/2010/09/27/us/27wiretap.html.

178. *Id.*

179. *Id.*

180. *Id.*

181. *Net Encryption Backdoors*, *supra* note 175.

182. Savage, *supra* note 177.

183. *Id.*

184. *Id.*

185. *Id*

186. Mate, *supra* note 44, at 219.

on the strength of the British parliamentary system.[187] Although there are elements of limited government embodied in the Constitution's Fundamental Rights section, the removal of a due process clause greatly weakened the power of Indian courts to challenge governmental actions.[188] With this, "the [Indian] Constitutional Assembly . . . subordinate[d] key provisions . . . [of] fundamental rights to larger social goals of preserving order and morality."[189]

"[T]he Indian Constitution was also shaped and influenced by a distinctly socialist ideology and worldview that had been championed by [Prime Minister] Nehru and other leaders of the Congress party."[190] As amended in 1976, the Indian Constitution opens with the inaugurate statement: "WE, THE PEOPLE OF INDIA, having solemnly resolved to constitute India into a [SOVEREIGN SOCIALIST SECULAR DEMOCRATIC REPUBLIC] . . . ."[191] This preamble evidences that "[t]he foundation of [India's] social philosophy was the evolution of a secular socialist democracy . . . ."[192]

The socialist philosophy of India has been a consistent obstacle for advocates of freedom and fundamental rights. Influenced by a tradition of "positivist jurisprudence in England," the framers of the Indian Constitution established a subservient judiciary.[193] Constitutional authors "envisioned a Court that would not interfere with Parliament's power to enact policies that would effect a collectivist, socialist transformation."[194] Although the Indian Constitution established a Supreme Court with the power of judicial review, the Constituent Assembly prevented judicial activism in the realm of civil liberties by omitting a due process clause.[195]

---

187. *Id.* at 224.

188. *Id.*

189. *Id.* at 219.

190. *Id.* at 226. Prime Minister Nehru once remarked that "[socialism] is a vital creed which I hold with all my head and heart." Jawaharlal Nehru, *Presidential Address to the National Congress, 1936*, *in* INDIA AND THE WORLD: ESSAYS 83 (H.G.A. ed., 1936).

191. INDIA CONST. pmbl., *amended by* The Constitution (Forty-Second Amendment) Act, 1976. Passed by the Indian Parliament on November 2, 1976 (during the Emergency Era), the Forty-Second Amendment "changed the characterization of India to [a] 'sovereign, socialist secular democratic republic' from [a] 'sovereign democratic republic.'" Prateek Deol, *42nd Constitutional Amendment: A Draconian Parliament*, LEGAL SERVICE INDIA (Oct. 9, 2007), http://www.legalserviceindia.com/articles/editorial.htm. This Amendment greatly reflects Indian ideology and its effect on the composition of the Constitution. *Id.* The Amendment served four major purposes: 1) to "[e]xclude the courts entirely from election disputes;" 2) "[t]o strengthen the central government vis-à-vis the state governments and its Compatibility to rule the country as a unitary, not a federal, system;" 3) "[t]o give maximum protection from judicial challenge to social revolutionary legislation;" and 4) "to trim the judiciary, so as to "make it difficult for the court to upset parliament's policy in regard to many matters." *Id.*

192. V.R. Krishna Iyer, *Nehru Revisited*, THE HINDU (Nov. 18, 2001), *available at* http://www.hinduonnet.com/thehindu/mag/2001/11/18/stories/2001111800070400.htm.

193. Mate, *supra* note 44, at 254.

194. *Id.*

195. *Id.* at 219.

B. Article 21 Analysis

Article 21 of the Indian Constitution establishes the civil liberty derivative found in the Fifth Amendment of the U.S. Constitution.[196] The Article states, "No person shall be deprived of his life or personal liberty except according to procedure established by law."[197] Although the Indian Constituent Assembly initially provided for due process in Article 21, the framers deliberately omitted "due process" from the Article's final draft, replacing this clause with "procedure established by law."[198] "The omission of the word[,] 'due,' the limitation imposed by the word[,] 'procedure[,]' and the insertion of the word[,] 'established[,]' [clearly reveals the] idea of legislative prescription."[199] By incorporating the phrase, "procedure established by law," the Indian Constitution grants final authority to the legislature.[200]

C. Emergence of Due Process

Despite the omission, the Indian judiciary adopted an activist approach to interpreting fundamental rights and effectively created new doctrines of due process and nonarbitrariness.[201] A series of ground breaking Indian Supreme Court cases have played a "significant role" in the development of certain enumerated rights,[202] including the right to privacy.

1. A.K. Gopalan v. State of Madras

In *A.K. Gopalan v. State of Madras*, the Indian Supreme Court meaningfully examined the Fundamental Rights provisions of the Constitution for the first time.[203] The important issue raised in *Gopalan* was whether the Preventive Detention Act of 1950 violated a citizen's fundamental rights under the Constitution.[204] This issue was unprecedented in post-revolutionary India;[205] thus, in order to affect a judgment, the Supreme Court considered alternative approaches to determine the scope of personal liberty provided by Article 21.[206]

Ultimately, Chief Justice Kania restricted the scope of fundamental rights

196. INDIA CONST. art. 21.
197. *Id.*
198. Mate, *supra* note 44, at 221-22.
199. *Id.* at 233.
200. *Id.*
201. Mate, *supra* note 44, at 217.
202. Nehaluddin Ahmad, *Privacy and the Indian Constitution: A Case Study of Encryption*, 7 COMM. IBIMA 8, 11 (2009).
203. A.K. Gopalan v. State of Madras, (1950) 1 S.C.R. 88, 95 (India).
204. *Id.* at 88.
205. Mate, *supra* note 44, at 226.
206. *Gopalan*, 1 S.C.R. at 89-92.

by reading these liberties in isolation from Article 21.[207] The Court interpreted "procedure established by law" to mean the law established by the State, that is to say, the Union Parliament or the Legislatures of the States.[208] "It is not proper to construe this expression in the light of the meaning given to the expression 'due process of law' in the [U.S.] Constitution by the [United States Supreme Court] . . . ."[209] Additionally, the Court explained that the word, "law," in the context of Article 21, did not mean the *jus naturale* of civil law but rather that of positive or state-enacted law.[210]

Although the *Gopalan* majority composed a restricted view of Article 21, in a dissenting opinion, Justice Fazl Ali considered a broader interpretation.[211] Justice Ali construed "procedure established by law" to encompass higher principles of natural law and justice.[212] In his opinion, Ali highlighted a series of decisions by the U.S. Supreme Court, in which that Court recognized the word, "law," to include fundamental principles of justice.[213] Despite Justice Ali's argument to incorporate procedural due process into the Indian Constitution, however, the majority asserted that Article 21 was not intended to incorporate principles of natural law and justice.[214] The *Gopalan* Court, though adopting a restricted view of fundamental rights, was the first panel to begin a discussion of the infusion of due process into the Indian Constitution.[215]

2. Kharak Singh v. State of Uttar Pradesh

In *Kharak Singh v. State of Uttar Pradesh*, the Indian Supreme Court first examined the right of privacy under the Indian Constitution.[216] The Court determined that, although the right to privacy was not expressly guaranteed in the Constitution, it was implicit in the fundamental rights of life and personal liberty under Article 21 and cannot be curtailed except according to a procedure established by law.[217] In *Singh*, the Court examined the constitutionality of a police surveillance regulation that addressed the practice of police shadowing.[218] Through this procedure of surveillance, police would supervise

207. *Id.* at 89.
208. *Id.* at 90.
209. *Id.*
210. *Id.* at 90-91.
211. *Id.* at 91.
212. *Id.* at 160-163.
213. *Id.*
214. *Id.* at 108.
215. Mate, *supra* note 44, at 226.
216. Kharak Singh v. State of Uttar Pradesh, (1964) 1 S.C.R. 332 (India); Rajagopal v. State of Tamil Nadu, (1994) 6 S.C.C. 632, 639 (India).
217. *Id.* at 359; *see also* Govind v. State of Madhya Pradesh, (1975) 3 S.C.R. 946, para. 14 (India) and *Rajagopal*, 6 S.C.C. at 639 (discussing *Singh*'s recognition of the right).
218. *Singh*, 1 S.C.R. at 333.

the actions and movements of citizens possessing criminal records.[219] Among the techniques permitted by the regulation, police were allowed to approach the houses of suspects and to make domiciliary visits at night.[220] Kharak Singh had a "class A" criminal history and was therefore subject to the gamut of police surveillance.[221] To determine whether Singh was at home one evening, police entered his house and disturbed his rest.[222] Singh brought suit to enjoin the police from intrusive surveillance techniques permitted by U.P. Police Regulation 236.[223]

The Court held the police regulation to be unconstitutional because it violated the fundamental rights guaranteed by Articles 19 and 21 of the Indian Constitution.[224] Coming to this conclusion, the Court examined the U.S. Supreme Court decision in *Wolf v. Colorado*.[225] There, Justice Frankfurter observed that "[t]he security of one's privacy against arbitrary intrusion by the police . . . is basic to a free society" and, therefore, "implicit in the concept of ordered liberty" under the Due Process Clause of the U.S. Constitution.[226] Echoing Justice Frankfurter's analysis, the *Singh* Court found: "It is true our Constitution does not expressly declare a right to privacy as a fundamental right, but the said right is an essential ingredient of personal liberty."[227]

3. Maneka Gandhi v. Union of India

The most significant development in the emergence of due process in India was the Court's decision in *Maneka Gandhi v. Union of India*.[228] In *Gandhi*, the Indian government impounded the passport of Maneka Gandhi pursuant to the Passport Act of 1967.[229] Having surrendered her passport, Gandhi was disabled from traveling outside the country.[230] When she requested the reason for the order, the Ministry of External Affairs responded that it was "in the interest of the general public."[231] Gandhi filed suit alleging that "[t]he right to [travel] abroad is part of 'personal liberty' within the meaning of . . . Article 21 and [that] no one can be deprived of this right except according to

219. *Id.*
220. *Id.* at 332.
221. *Id.* at 334.
222. *Id.*
223. *Id.* at 332.
224. *Id.* at 334.
225. *Id.* at 348; *see generally* Wolf v. Colorado, 338 U.S. 25 (1949).
226. *Singh*, 1 S.C.R. at 348 (quoting *Wolf*, 338 U.S. at 27).
227. *Id.* at 359.
228. Maneka Gandhi v. Union of India, (1978) 2 S.R.C. 621 (India). "In doctrinal terms, the *Maneka Gandhi* decision was ground-breaking . . . ." Mate, *supra* note 44, at 246.
229. *Gandhi*, 2 S.C.R. at 621.
230. *Id.*
231. *Id.*

the procedure prescribed by law."[232]

In its decision, the Court examined the scope of Article 21 and the constitutional meaning of "procedure established by law."[233] A six-judge majority expanded the scope of Article 21, holding that there was not a substantial difference between the phrase, "procedure established by law," under the Indian Constitution and the phrase, "due process of law," under the U.S. Constitution.[234] In so holding, the *Gandhi* Court decided that any procedure implicating the rights to life and liberty in Article 21 must be "right and just and fair."[235] In one of the most famous passages in Indian constitutional law, Justice Bhagwati references U.S. Supreme Court Justice Holmes in articulating the doctrine of nonarbitrariness:

> The principle of reasonableness[,] which legally as well as philosophically, is an essential element of equality or non-arbitrariness[,] pervades Article 14 like a brooding omni-presence and the procedure contemplated by Article 21 must answer the test of reasonableness in order to be in conformity with Article 14. It must be "right and just and fair" and not arbitrary, fanciful, or oppressive; otherwise it would be no procedure at all and the requirements of Article 21 would not be satisfied.[236]

The *Gandhi* opinion is revolutionary because it unites the particularist conception of Indian law with a "universalist legal aspiration of foreign precedent and transitional norms."[237]

D. Attempts to Compel Decryption

There is currently no law regulating encryption in India.[238] Although action has been taken to protect privacy in the digital age, encryption regulation "largely remains in the development stage."[239] During the inception of cyber-law legislation, the Indian Parliament "largely neglected the issue of privacy of personally identifiable information."[240] Encryption regulation remains primarily within the domain of defense.[241]

---

232. *Id.* at 622.
233. *See id.*
234. Mate, *supra* note 44, at 246.
235. *Gandhi*, 2 S.C.R. at 674.
236. *Id.*
237. Mate, *supra* note 44, at 249.
238. Ahmad, *supra* note 202, at 10.
239. *Id.* at 10-11.
240. *Id.* at 13.
241. *Id.* at 14.

1. Information Technology Act (2000)

On June 9, 2000, the Indian Parliament adopted the Information Technology Act of 2000 (ITA).[242] The purpose of this legislation was

> to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as 'electronic commerce', which involve the use of alternatives to paper-based methods of communication and storage of information, [and] to facilitate electronic filing of documents with the Government agencies.[243]

With this Act, the Indian Parliament sought to keep pace with international regulation of electronic commerce.[244] Recognizing that international e-commerce regulation had begun decades prior, at least one commentator has remarked that "it's better late than never."[245]

The ITA introduced the first legislative control of encryption communication in India.[246] The Act establishes a system of regulation for the recording and authentication of encryption certificates.[247] The ITA imposes stringent duties on digital signature subscribers.[248] Encryption users must surrender their public encryption key to a certifying authority and apply for a digital signature certificate.[249] Additionally, every subscriber is directed to exercise reasonable care to retain control of their private encryption key and must report if the code has been compromised.[250]

With the adoption of the ITA, the Indian government created the office of the Controller of Certifying Authorities (Controller).[251] The Controller is appointed by the central government and exercises broad discretionary authority over encryption certification agencies.[252] Included in this authority, is the power

242. Information Technology Act, No. 21 of 2000, INDIA CODE (2000).

243. *Id.* pmbl.

244. Aashit Shah, *The Information Technology Act, 2000: A Legal Framework for E-Governance*, SUDHIRLAW.COM, http://www.sudhirlaw.com/cyberlaw-itact.htm (last visited Mar. 25, 2012).

245. *Id.*

246. Ahmad, *supra* note 202, at 14.

247. *Id.*

248. Information Technology Act, No. 21 of 2000, INDIA CODE (2000), §§ 40-42. A "subscriber" is the "person in whose name the Digital Signature Certificate is issued." *Id.* § 2(1)(zg). Digital Signature Certificates are issued by Certifying Authorities verifying that a subscriber's encryption key is secure and authentic. *See Id.* § 36.

249. *Id.* §§ 40, 41.

250. *Id.* § 42.

251. *Id.* § 17(1).

252. *Id.* §§ 17, 18.

to direct a government agency to intercept any encrypted communication.[253] The Act provides:

> If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign [States] or public order or for preventing incitement to the commission of any cognizable offence . . . direct any agency of the Government to intercept any information transmitted through any computer resource.[254]

Once a subscriber's communication has been intercepted, he is called upon to "extend all facilities and technical assistance to decrypt the information."[255] If the person fails to comply with this order, he may be punished with imprisonment for up to seven years.[256]

By prohibiting the Controller direct access to private encryption keys, the Indian government sought to preserve the integral right of privacy "flowing from Article 21 of the Constitution."[257] However, the Controller is granted broad discretionary authority to determine when a transmission may be intercepted.[258] It has been argued that this procedural safeguard is not adequate to protect the right of privacy.[259] By requiring mandatory cooperation for the submission of private encryption keys (without the guarantee of due process), Parliament has functionally removed the freedom of encrypted communication.

2. Prevention of Terrorism Act (2002)

"In March 2002 the Indian Parliament . . . passed the Prevention of Terrorism Act (POTA) over the objections of several [o]pposition parties and in the face of considerable public criticism."[260] The regulation codifies the Prevention of Terrorism Ordinance, which was built upon the Terrorists And Disruptive Activities (Prevention) Act.[261] POTA gives law enforcement sweeping powers to arrest suspected terrorists, intercept communications, and

253. *Id.* § 69(1).
254. *Id.*
255. *Id.* § 69(2).
256. *Id.* § 69(3).
257. Ahmad, *supra* note 202, at 14.
258. Information Technology Act, No. 21 of 2000, INDIA CODE (2000), § 69(1).
259. Ahmad, *supra* note 202, at 14-15.
260. *The Republic of India*, PRIVACY INT'L (Nov. 16, 2004), *available at* https://www.privacyinternational.org/reports/india.
261. *Id.*; *see generally* The Prevention of Terrorism Ordinance, No. 9 of 2001, INDIA CODE (2001); The Terrorists And Disruptive Activities (Prevention) Act, No. 28 of 1987, INDIA CODE (1987).

curtail free expression.[262]

Chapter Five of POTA enables a police officer (not below the rank of Superintendent) supervising the investigation of a terrorist to intercept any wire, electronic, or oral communication if he believes that such communication may provide evidence of an offense involving terrorism.[263] Although the necessity of interception is determined at the discretion of the supervising officer, the interception must be approved by a government-appointed Competent Authority through the authorization of an application.[264] Similar to a search warrant in the United States, the application must contain "a statement of the facts and circumstances relied upon by the applicant to justify his belief that an order should be issued," including specific details and description of the offense.[265] As an additional measure of accountability, every application is subject to review by the central government.[266] If the Review Committee disapproves an application for interception, the intercepted communication shall be destroyed and the information shall not be admissible against the accused at trial.[267] However, critics of the system of judicial review and parliamentary oversight believe that it remains to be seen how effective such mechanisms will be in practice.[268]

Upon the authorization of an application for interception, the investigating officer is authorized to direct the provider of an electronic communication service to furnish "all information, facilities and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference . . . ."[269] If the intercepted electronic communication is encrypted, cooperation with the Act would require the submission of an encryption code. Additionally, information intercepted pursuant to the requirements of the Act shall be admissible as evidence against the accused at trial.[270]

Notwithstanding the customary application requirements, POTA authorizes an unwarranted interception in emergency situations.[271] Recognized emergency situations include the "immediate danger of death or serious physical injury to any person" and "conspiratorial activities threatening the security or interest of the State."[272] Furthermore, "[i]n certain high-risk states

262. *See* The Prevention of Terrorism Act, No. 15 of 2002, INDIA CODE (2002).
263. *Id.* § 38(1).
264. *Id.* §§ 37, 38.
265. *Id.* § 38(2)(b).
266. *Id.* § 46.
267. *Id.* § 46(4).
268. Tariq Ahmad Bhat, *Kashmir: Booth Capture Ban on Long Distance Calls Affects Business,* THE WEEK (Mar. 17, 2002), http://www.theweek.com/22mar17/events9.htm.
269. The Prevention of Terrorism Act, No. 15 of 2002, INDIA CODE (2002), § 40(2).
270. *Id.* § 45.
271. *Id.* § 43.
272. *Id.* § 43(1)(a)(i), (ii).

such as Jammu and Kashmir, search warrants are not required."[273] These local governments can also indiscriminately ban the use of cell phones and cybercafés.[274]

POTA represents an effective example of non-arbitrary legislation addressing, among other things, the interception of electronic communications.[275] Encryption regulation is implicit in the compliance provision of Chapter Five.[276] The Act is specific in its purpose and establishes a system of parliamentary supervision and judicial review of the powers granted within.[277] On its face, the Act effectively authorizes necessary state action for the protection against terrorism while maintaining the constitutional guarantees of liberty and privacy. This legislation represents a "procedure established by law," which, if determined to be non-arbitrary, is a constitutional exercise of the regulation of electronic communication in India. However, as evidenced by the exceptions, the Act does not have universal application.[278] The Indian government has allowed the unwarranted seizure of suspect communications only in times of emergency or areas of high risk.[279]

V. RECOMMENDATIONS

A. Non-Arbitrary Legislation

As evidenced by continuous legislative activity, encryption regulation, like all other forms of technology-driven legislation, is an ongoing process. Undoubtedly, keeping pace with a quickly evolving market of electronic communications is a daunting task. It may be for this reason that the U.S. Congress and the Indian Parliament have proposed broad legislation intended to flexibly accommodate those changing needs. However, overly broad and vague legislation will almost certainly face constitutional scrutiny upon judicial review. Additionally, it is procedurally and politically difficult to adopt sweeping legislation that seeks to achieve a broad legislative purpose. Encryption regulation is especially subject to these complications.

In lieu of this legislative challenge, effective encryption regulation must be direct, specific, and non-arbitrary. In both the United States and India, provisions regulating the use of encryption have generally been included in broader regulatory schemes.[280] To ensure constitutional validity, Congress and

273. *The Republic of India*, *supra* note 260.
274. *Id.*
275. *See* The Prevention of Terrorism Act, No. 15 of 2002, INDIA CODE (2002), ch. 5.
276. *See id.* § 40.
277. *See id.* § 46(4).
278. *The Republic of India*, *supra* note 260.
279. *Id.*
280. *See supra* Parts III.E, IV.D.

Parliament must examine encryption control in isolation. A strong example of directed legislation is China's Regulations on the Administration of Commercial Cipher Codes.[281] The Chinese government enacted these rules to "strengthen the administration of commercial encryption, to protect the security of information, to protect the lawful rights and interests of citizens and organizations and to safeguard State security and interests."[282] Combined, these constitute a clear and specific purpose that may effectively support directed legislation.[283] "China's approach to encryption differs markedly from the international practice, by handling encryption as a unified policy, under the direct supervision of Chinese leadership, encompassing both state and commercial security applications."[284]

"'China really has an enthusiasm for regulation and standardization that is unmatched anywhere else in the world.'"[285] With this legislation the Chinese government set standards for the research, manufacture, distribution, import and export, use, security, and storage of encryption products.[286] Admittedly, the stringent approach adopted by the Chinese is not a model structure, but rather it serves as an example of an overly restrictive approach against which the U.S. and Indian governments should measure their efforts.

B. Password Management Agencies

As evidenced by the U.S. telecommunications industry's noncompliant response to CALEA, legislation alone, whether arbitrary or not, has been insufficient to achieve effective encryption control.[287] Some critics believe the problem results from an abuse of discretion by law enforcement,[288] while others argue for the necessity of judicial review.[289] Addressing these concerns may assist in resolving procedural concerns, but successful regulation will not be accomplished without industry compliance. When CALEA was adopted, it was primarily industry associations and consumer-rights organizations that

281. Shangyong Mima Guanli Tiaoli (商用密码管理条例) [Regulations on the Administration of Commercial Cipher Codes] (promulgated by the State Council, Oct. 7, 1999, effective Oct. 7, 1999) (China).

282. *Id.* art. 1.

283. *See* Part IV.C.3.

284. *IT Security - Chinese Standards Deviating from Existing International Standards and Global Practices*, MARKET ACCESS DATABASE, http://madb.europa.eu/madb_barriers/barriers_details.htm?barrier_id=085196&version=2 (last updated Nov. 15, 2011).

285. Ellen Messmer, *Encryption Restrictions*, NETWORKWORLD (Mar. 14, 2004), http://www.networkworld.com/careers/2004/0315man.html?page=1.

286. *IT Security - Chinese Standards Deviating from Existing International Standards and Global Practices*, *supra* note 284.

287. *See supra* Part III.E.3.

288. *See* Palfreyman, *supra* note 19, at 375.

289. *See* Ungberg, *supra* note 108, at 556.

vigorously opposed the law.[290] This resulted from the industry's technical inability to alter its operating systems without substantial cost.[291] Therefore, the success of new legislation seeking similar objectives cannot be the result of a technical solution. Requiring the industry to change the design and performance of its products will result in unwanted consequences. First, it has the potential to stifle innovation. Designers would have to operate within the parameters of the regulation and will be limited in creativity and innovation. Second, it has potential to harm Internet functionality. A rule requiring a technical change may substantially alter the architecture of the system. Last, any success will be short-lived. If the government restricts the operation and performance of digital encryption devices, tech-savvy engineers will inevitably find a way around it, creating a black market of encryption technology that the government will have more difficulty controlling.

The solution is the development of password management agencies. These agencies should be similar to the certified authorities created in India's Information Technology Act[292] or the agencies established in China's Regulations for the Administration of Commercial Cipher Codes.[293] Under this system, when a digital encryption device is imported or manufactured, the private encryption codes must be surrendered to a certified password management agency. Therefore, by the time an encryption product is sold to a business or consumer, the password agency will have already archived the encryption key. Password management agencies will have a stringent obligation to protect the archived encryption codes with the utmost security, perhaps even through further encryption.

Retrieval of an individual's encryption key must be accomplished by obtaining a warrant. Traditional search warrant requirements should apply to ensure the protection of citizens' constitutional rights. However, the traditional warrant exceptions should not apply. The implementation of exceptions will render the warrant requirement arbitrary. Moreover, the safety and preservation policy concerns that support traditional search warrant exceptions do not exist in the recovery of encryption keys.

VI. CONCLUSION

The U.S. Constitution guarantees the fundamental right of liberty for all its citizens. The freedom of encryption is implicated by this unalienable right.

290. Jared Bazzy, *CALEA Deep in Court Quagmire*, 35 TELECOMM. 16 (2001). Among the CALEA challengers are USTA (United States Telephone Association), CTIA (Cellular Telecommunications and Internet Association), PCIA (Personal Communications Industry Association), ACLU (American Civil Liberties Union), and EFF (Electronic Frontier Foundation). *Id.*

291. *Id.*

292. *See supra* Part IV.D.1.

293. *See supra* Part V.A.

The Fourth and Fifth Amendments articulate freedom against compelled decryption: the Fourth Amendment protects individuals from the unwarranted seizure of an encryption code,[294] while the Fifth Amendment privilege against self-incrimination prevents the mandatory production of an encryption key when production would be testimonial.[295] Although attempts have been made, compelled decryption in the United States has ultimately failed.[296] This result is not a product of constitutional protections alone, but rather it reflects the implicit U.S. philosophy of freedom.[297]

Similar to the civil liberties established in the U.S. Constitution's Bill of Rights, the Indian Constitution promulgated fundamental rights for its citizens.[298] Article 21 articulates individual protections against the central government.[299] The constitutional examination of encryption regulation in India begins with this Article. Although the Indian Supreme Court has advocated for individual freedom under Article 21, the judiciary has continually supported the concept that individual privacy must remain subservient to national interests and national security.[300] Exemplifying this ideology, Dr. Nehaluddin Ahmad asserts that, although the right to privacy has been recognized as inherent in the right to life with dignity under Article 21, this right "should [not] be allowed to stand as an impediment in curbing activities prejudicial to national security interests."[301] Nevertheless, compelled decryption in India has been unsuccessful.[302] As in the United States, however, this failure is not a result of constitutional objection; the challenges have originated in non-constitutional matters, such as third-party negotiations. But because India reveres the power of central government, mandatory encryption production may eventually become a reality.

294. *See supra* Part III.B.
295. *See supra* Part III.C.
296. *See supra* Part III.D.
297. *See supra* Part III.A.
298. *See* INDIA CONST. art. 21.
299. *Id.*
300. Ahmad, *supra* note 202, at 15.
301. *Id.* at 15.
302. *See supra* Part IV.D.