2 Va. J.L. & Tech. 2 (Fall 1997) <http://vjolt.student.virginia.edu>
1522-1687 / © 1997 Virginia Journal of Law and Technology Association

VIRGINIA JOURNAL of LAW and TECHNOLOGY

| UNIVERSITY OF VIRGINIA | FALL 1997 | 2 VA. J.L. & TECH. 2 |
|---|---|---|

# The Use of Encrypted, Coded and Secret Communications is an "Ancient Liberty" Protected by the United States Constitution

by John A. Fraser, III[*]

---

# I. Introduction

1. In this electronic and digital age, the ability of a speaker and a selected audience to communicate in confidence about subjects chosen by them may be critical to the survival of free speech and privacy.[1] It is the primary purpose of this paper to demonstrate that, from the early years of the American Republic, Americans have enjoyed a robust, free, and frequent use of codes, ciphers, and other forms of secret communication.[2] Secondarily, this paper will demonstrate that Americans have long used secret modes of communication for numerous purposes, including political dissent, preservation of personal privacy in intimate matters, commerce, and criminal enterprises.[3]
2. 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. Encryption was speech. American history since the adoption of the Bill of Rights in 1791 demonstrates a continued use of encryption for many purposes. Based on this history, the concluding section of the paper briefly summarizes the arguments for protecting the continued use of secret modes of communication under the United States Constitution.[4] Although there are weighty law enforcement and national security interests at stake, the freedoms of the Founding Generation should not be eroded by continued technological advances in electronics.[5]

# II. The Constitution Protects Ancient Liberties

### A. An Overview of Ancient Liberties in Communications and Expression

3. As part of the Twentieth Century process of incorporating almost all of the Bill of Rights in the Fourteenth Amendment of the United States Constitution, the Supreme Court has repeatedly examined and studied the history of a number of social practices and customs. Those practices and customs that the Court has recognized as deserving of constitutional protection have at times been characterized as "fundamental," or "essential" to "ordered liberty."[6] For present purposes, it is necessary to restrict review of the Supreme Court cases to those cases that deal with expression and communication, and to further restrict review to those cases that explicitly rely for a portion of their analysis on the historical customs and practices of Americans. Because one of the earliest of these cases expressly held that taking to the streets and sidewalks for discussion and debate is an

"ancient liberty,"[7] this paper refers to these cases as the "Ancient Liberty" cases.

4. The cases that recognize and define ancient liberties in communications and expression rely for their historical strengths on the practices and intentions of the Founding Generation, on British legal traditions, and on the historical customs and practices of the people of the United States. In the context of communications and expression, the "ancient" liberties recognized by the Court include the use of sidewalks and streets for discussion of matters of public concern,[8] outdoor distribution of leaflets,[9] door-to-door political or religious canvassing,[10] picketing,[11] public demonstrations and parades,[12] boycotts,[13] newspaper publication on matters of public interest,[14] printing and distribution of caricature and parody of public figures,[15] and posting of signs on private property.[16] In 1923, the Supreme Court also recognized as "fundamental" the right to speak and teach foreign languages to children, even in wartime.[17]

**B. *McIntyre v. Ohio Elections Commission***

5. That the social and legal history of the United States plays an important role in determining what is an Ancient Liberty is evidenced on the face of the opinions of the Supreme Court cited above. British and American historical experiences inform the meaning of the Constitution by providing context for some practices (*e.g.*, anonymous speech) and in some cases, appear to provide the controlling rationale for Court majorities (*e.g.*, public figure caricatures and residential signs). However, the relevance of historical materials for Constitutional adjudication is perhaps best illustrated by the recent decision of the Supreme Court in *McIntyre v. Ohio Elections Commission*.[18] In that case, Mrs. McIntyre distributed leaflets at public meetings.[19] Some of the leaflets were not signed, but all of them opposed the expenditure of further funds on public schools in Westerville, Ohio. Mrs. McIntyre was convicted of a misdemeanor, having violated an Ohio Elections Code that prohibited anonymous election literature.[20]
6. In the Supreme Court, the Ohio Code provision that prohibited anonymous election leaflets was held to violate the First and Fourteenth Amendments. Justice Stevens, joined by four other justices, briefly canvassed the history of anonymous literature, including Shakespeare, Mark Twain, George Eliot, the Federalist Papers and other American Revolutionary-era political writings as part of the analysis of what types of expression are protected against content-based regulation.[21] The final holding is based on a plain historical judgment:

> Under our Constitution, anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent. Anonymity is a shield from the tyranny of the majority. See generally J. Mill, On Liberty and Considerations on Representative Government 1, 3-4 (R. McCallum ed. 1947) It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation--and their ideas from suppression--at the hand of an intolerant society. The right to remain anonymous may be abused when it shields fraudulent conduct. But political speech by its nature will sometimes have unpalatable consequences, and, in general, our society accords greater weight to the value of free speech than to the dangers of its misuse. See *Abrams v. United States*, 250 U.S. 616, 630-31 (1919) (Holmes, J., dissenting). Ohio has not shown that its interest in preventing the misuse of

anonymous election-related speech justifies a prohibition of all uses of that speech. The State may, and does, punish fraud directly. But it cannot seek to punish fraud indirectly by indiscriminately outlawing a category of speech, based on its content, with no necessary relationship to the danger sought to be prevented. One would be hard pressed to think of a better example of the pitfalls of Ohio's blunderbuss approach than the facts of the case before us.[22]

7. The *McIntyre* majority opinion demonstrates that at least five Justices of the Supreme Court believe that the historical background of the type of expression that is regulated is an important element in determining whether the type of expression is protected by the Constitution. In her concurring opinion, Justice Ginsburg characterized the majority's decision as overturning a State action that was "unnecessary, overintrusive, and inconsistent with American ideals."[23] Although brief, this statement can fairly be read as supporting the majority's reliance on the history of anonymous speech as an important element in determining that the speech deserved Constitutional protection.
8. Justice Thomas, concurring in *McIntyre*, pursued his particular understanding of the original intent of the Framers of the Constitution.[24] History is not just important to Justice Thomas in Constitutional cases; it is a critical element of analysis of the original understanding, which understanding controls the outcome of the case.[25] Specifically, Justice Thomas holds that it is necessary to search through the various authoritative materials available to determine what the specific practices, beliefs, and statements of the Framers were in regard to anonymous speech.[26] Under the original intent jurisprudence followed by Justice Thomas, the absence of a direct indication from the Framers on the precise issue before the Court leads to a second question: what does history reveal as the "contemporaneous understanding" of the Constitutional provision that is at issue.[27]
9. Following the analytical framework just outlined, Justice Thomas' concurring opinion in *McIntyre* indicates that there is no record of "discussions of anonymous political expression either in the First Congress, which drafted the Bill of Rights, or in the state ratifying conventions. Thus, our analysis must focus on the practices and beliefs held by the Founders concerning anonymous political articles and pamphlets."[28] The review then conducted in pursuit of the original intent of the Founders ranges across a wide array of historical materials, including matters from before the American Revolution,[29] acts of important members of the Continental Congress and state officials during the Revolutionary period,[30] and the expressed opinions of both Federalist and Anti-Federalist editors on the subject of anonymous articles during the fight over ratification of the Constitution.[31] Justice Thomas finds compelling proof in the Framers' "universal practice of publishing anonymous articles and pamphlets, [indicating] that the Framers shared the belief that such activity was firmly part of the freedom of the press. It is only an innovation of modern times that has permitted the regulation of anonymous speech."[32]
10. Justice Thomas states that the "record is not as complete or as full as [he] would desire."[33] Additional, persuasive materials that are lacking include Federal government actions after the adoption of the Bill of Rights and early court cases interpreting the First Amendment in the context of anonymous speech. However, the picture is completed for Justice Thomas, to the extent possible, by a review of the practice of using anonymous political literature during the first

elections under the new Constitution, anonymous printed debates between Alexander Hamilton and James Madison over foreign policy, and continued publication of anonymous political materials in the press through the election of Thomas Jefferson as President in 1800.[34]

11. Because of the proofs adduced, Justice Thomas finds that there is no ambiguity in the original intent of the framers in regard to anonymous political pamphlets. He criticizes the majority for considering the anonymous nature of the works of Voltaire and George Eliot--characterizing the majority's inquiry into such as "irrelevant."[35] He also rejects the majority's assignment of "value" to anonymous political speech, holding that "what *is* important is whether the Framers in 1791 believed anonymous speech sufficiently valuable to deserve the protection of the Bill of Rights."[36] Justice Thomas concurred only in the judgment because the majority adopted "an analysis that is largely unconnected to the Constitution's text and history."[37]
12. Justice Scalia was the lone dissenter. Although Justice Scalia's dissenting opinion begins with a defense of the original intent school of jurisprudence,[38] the opinion labels the historical materials of the majority and of Justice Thomas' concurrence as not addressed to the issue before the Court.[39] Characterizing the issue as "the most difficult case for determining the meaning of the Constitution" because of a lack of appropriate historical materials, Justice Scalia argues that deference should be given to the state legislators and politicians who have passed laws in every state restricting anonymous pamphleteering.[40]
13. Thus, as evidenced by *McIntyre,* every Justice of the Supreme Court regards the Eighteenth Century treatment and use of a type of expression as bearing more or less directly on the issue of whether that type of expression will be protected under the Constitution. This is consistent with the "Ancient Liberty" line of cases discussed above, in which the Court has relied on history to analyze and define the scope of Constitutional protection for communication and expression.
14. Moreover, for two of the Justices and Chief Justice Rehnquist, historical materials that indicate the precise opinion of the Framers on the matter before the Court can provide the *ratio decidendi* for the case. Chief Justice Rehnquist has written a number of original intent opinions, including *Hustler Magazine v. Falwell*, 485 U.S. 46 (1988). Justice Scalia's jurisprudence requires that the opinion expressed by a member of the founding generation be directly on point, indistinguishable in all material respects from the case at bar. Justice Thomas is willing to judge the original intent from what the Framers did as well as what they said.

**C. Significance of the Ancient Liberty Cases**

15. *McIntyre* continues a long tradition of using historical evidence from the Colonial, Revolutionary, and Ratification eras, as supplemented by the later history of the United States, to inform Constitutional adjudication affecting rights of communication and expression.[41] Any litigant or scholar preparing to address the Constitutional status of a type of expression would be well-advised to research and analyze the acts and statements of the Founders in regard to that type of expression.
16. The "Ancient Liberty" cases touching on freedom of expression or communication contribute at least two important rules to Constitutional jurisprudence and litigation. In general First Amendment jurisprudence, it is important to categorize regulated behavior as speech or conduct.

Government is generally permitted to regulate conduct, and the "rational basis" test is the standard of review applied to regulations intended to affect conduct.[42] Once behavior is categorized as "speech," regulation of that behavior is reviewed under either a "strict scrutiny" or "intermediate" standard of review.[43] However, the speech/conduct dichotomy does not seem to be important once a mode of expression is determined to have been in use at the time the Constitution was adopted, or the Bill of Rights was ratified.[44] Supreme Court majorities rely on the "ancient" nature of some types of expression in order to avoid the speech/conduct dichotomy.[45] What may appear to be conduct in some respects may actually be an ancient liberty, long employed by the people for expression of their viewpoints. The speech versus conduct dichotomy is pushed to the side when this is demonstrated.[46]

17. The second contribution of this group of cases is that, as a result of seventy years of accretion, a rule of law can be recognized. At the very least, the Constitution protects all forms or types of expression or communication[47] that meet the following three-part test.[48] Those modes of expression or communication are protected which (1) are historically demonstrated to have been in widespread use as of the adoption of the Bill of Rights; which (2) are shown to have been sanctioned in use by the Framers of the Constitution and the Bill of Rights; and which (3) are shown to have long continued in use. Those modes of expression or communication which meet this three-part test may not be prohibited to the people, and may only be regulated when they are abused to accomplish some otherwise illegal purpose.[49]

## III. Secret Communication Methods Were in Widespread Use Prior to Ratification of the Bill of Rights

### A. Seventeenth and Eighteenth Century Britain and Colonial America

18. Secret communication methods were widely used in Seventeenth and Eighteenth Century England. When David Shulman published *An Annotated Bibliography of Cryptography*,[50] he listed a number of treatises on cryptographic subjects published in England between 1593 and 1776, as well as scholarly books that contained chapters on use of codes, ciphers, and secret writing techniques.[51] One treatise (John Wilkins' *Mercury, or the Secret and Swift Messenger)* can serve as an example of the widespread knowledge of various techniques of concealment of a message.[52] Wilkins described the use of parables of scripture, inversion of known words, secret inks and papers, changing the place of common letters, use of keys, double alphabets, invented characters, emblems, hieroglyphics, the use of tones and musical notes, as well as fire and smoke signals.[53]
19. It is not surprising that the printing press brought about the publication of so many treatises on encryption and closely related subjects. According to one major history of the cryptographic science, a number of prominent figures in British history used ciphers. These included Roger Bacon, Geoffrey Chaucer, and Mary Queen of Scots.[54] The House of Lords was sufficiently familiar with ciphers that it allowed the introduction of deciphered writings in the 1723 trial of Bishop Francis Atterbury.[55] The Royal Mail was so familiar with private and diplomatic ciphers

that, by 1720 in London, it operated one of the most sophisticated overnight systems of opening and deciphering mail.[56] Samuel Pepys, the noted diarist, used a very complex cipher technique in his late Seventeenth and early Eighteenth Century diaries, a method so complex that the key was not discovered until the Twentieth Century.[57]

20. In Colonial America, secret communications were used to defeat the efforts of government agents and social censors. Before 1700, John and Mary Winthrop of Puritan Massachusetts corresponded in a private cipher regarding intimate matters, thus concealing their affairs from persons who might read their messages while in the process of transmission by hand.[58] In 1748, George Fisher wrote, and Benjamin Franklin printed, an early American text on the uses of codes, ciphers, and secret writing to communicate only to the intended audience.[59] Because of the government practice of opening and reading private mail, and because mail might be stolen from the post riders, there was a substantial risk of exposure in colonial America.[60] In 1764, a young Thomas Jefferson suggested to John Page the use of a hundred-year-old English text (Shelton's *Tachygraphia*) to encode their letters to protect information about Jefferson's unsuccessful efforts to court a young lady.[61] When it was decided by a generation of revolutionaries to establish Committees of Secret Correspondence in all the colonies, which Committees acted in concert to oppose the Stamp Act of 1765, there was no shortage of knowledge about ways in which to maintain secret communications.[62]

**B. The American Revolution and the Founding Generation: 1775-1783**

21. From the beginnings of the American Revolution in 1775 until the adoption of the United States Constitution, Americans used codes, ciphers and other secret writings to foment, support, and carry to completion a rebellion against the British government. In the words of one author, "America was born of revolutionary conspiracy."[63] Moreover, "[a]s rebels and conspirators, the young nation's leaders ... turned to codes and ciphers in an effort to preserve the confidentiality of their communications."[64] Americans also continued to use secret communications methods for purely private correspondence, and for political correspondence where a restricted audience was desired.[65] The leading lights of the Revolution and the founding generation were frequent users of secret communications during the Revolution.[66]
22. George Washington, as commander of the Continental Army, was forced to deal with encryption and espionage issues shortly after taking command of the Army when it was conducting a siege of the British forces in Boston.[67] Benjamin Church, who was a trusted patriot, was caught corresponding with a British officer within the siege lines, and Washington was able to extract a confession only after having the correspondence decrypted by a local cipher expert.[68] Washington also was forced, through the circumstances of the War, to deal with encryption and decryption issues on a constant basis.[69] For example, he dealt with treasonous use of ciphers by Benedict Arnold in Arnold's unsuccessful effort to betray West Point,[70] and worked for years with Colonel Benjamin Tallmadge to obtain and conceal secret information from the British garrison in New York City.[71] Lord Cornwallis' messages were at times intercepted and deciphered for Washington.[72]

23. John Adams was a Revolutionary War leader from Massachusetts, member of the Continental Congress, diplomat, and second President of the United States. John and Abigail Adams, his wife, used a cipher provided by James Lovell for family correspondence while John Adams was away from home.[73] Notable among the Adams correspondence is a June 17, 1782 letter from Abigail Adams to John Adams in Paris, where he was in possession of a Lovell cipher. Abigail urged John to use the cipher to convey more confidential information to her, and she said that she used it with success.[74] The editor of the *Adams Family Correspondence* concluded that the Adamses used ciphers due to the dangers of interception of correspondence and the need to convey information in confidence.[75]
24. Thomas Jefferson was the author of the Virginia Declaration of the Rights of Man, author of the Declaration of Independence, Member of the Continental Congress, Minister to France, Secretary of State, President of the United States, and Founder of the University of Virginia. During the Revolution, Jefferson frequently made recourse to encrypted communications to protect his private thoughts, to convey confidential information, and to protect valuable political insights from prying eyes.[76]
25. James Monroe was a diplomat, Member of Congress, Secretary of State, and President of the United States, among other accomplishments. Monroe took a cipher with him to Paris in 1803, and used the cipher to communicate with Jefferson regarding the progress of negotiations concerning the Louisiana Purchase.[77] A number of the codes that he used in communicating with Jefferson and others have survived.[78]
26. James Madison was a close confidant of Thomas Jefferson, Member of the Constitutional Convention, Member of Congress, author of the Bill of Rights, diplomat, Secretary of State, and President. He was also a frequent and extensive user of secret communications during the Revolution, utilizing a number of different ciphers for private correspondence, correspondence with state officials in Virginia, and correspondence with fellow actors in the Revolution. Madison corresponded with Philip Mazzei, and withheld certain information due to lack of a cipher, in 1780 and 1781.[79] The Madison correspondence also includes numerous examples from the Revolutionary era of enciphered communications with state officials in Virginia and correspondence about the need for ciphers.[80] Madison corresponded extensively with Edmund Randolph on matters private and political, and they frequently resorted to encrypted writings to protect their secrets from robbery of the mails and to allow them to express opinions about individuals without fear of disclosure.[81] On one occasion, Madison was unable to supply information to Randolph due to the lack of a cipher for the correspondence.[82]
27. John Jay became first Chief Justice of the United States Supreme Court after a distinguished career as an attorney, statesman, and diplomat during and after the Revolution.[83] Jay used a secret code as early as October 1779,[84] and he used a secret code to correspond, evidently on personal matters, while on government business in Europe, and was required to use a cipher for all significant diplomatic correspondence.[85] Jay was instrumental early in the Revolution in obtaining "secret ink" from his brother James in London. James Jay warned the Americans of General Burgoyne's intended invasion from Canada, using the same ink.[86]
28. Benjamin Harrison was a member of the Virginia House of Burgesses, Member of the Continental Congress (where he served on the Committee of Correspondence), and Governor of Virginia

during the Revolution, among other duties.[87] The "nomenclator" used by Harrison for correspondence with Madison and others has survived in the Virginia records, and much of the correspondence has been deciphered.[88]

29. Edmund Randolph served the United States as Attorney General, Secretary of State, and as a Member of the Continental Congress and the Constitutional Convention. He served Virginia in a number of offices, including that of Governor.[89] Randolph and Madison conducted an extensive encrypted correspondence on private matters over a number of years.[90]
30. William Lee was a merchant, diplomat, Sheriff and Alderman of the City of London, and Commercial Agent for the Continental Congress in England, and was the brother of Arthur and Richard Henry Lee, discussed *infra.* [91] For correspondence between the brothers, a dictionary code was used.[92]
31. Arthur Lee received his M.D. degree from the University of Edinburgh and returned to Virginia, where he was elected as a Member of the Continental Congress, from which in turn he was sent as a diplomat to France and Berlin.[93] While in Europe, Arthur Lee's encrypted correspondence and reports were repeatedly stolen or reviewed in transit by British espionage officers.[94]
32. Richard Henry Lee, the third Lee brother in this paper, was a diplomat, Member of the Continental Congress, President of the Continental Congress, and United States Senator.[95] The Lee brothers' correspondence and their efforts to maintain secrecy are good examples of the wide knowledge and practical use of encryption from the Revolutionary era.[96] It should also be noted that the Lee brothers' enciphered correspondence remained unbroken until the 1920s, due to the complexity of the cipher.[97]
33. Benjamin Franklin was not only the printer of the 1748 text on ciphers cited above, but was also a prominent diplomat, supporter of the Revolution, and inventor of a "homophonic substitution cypher" while representing the United States in Paris in 1781.[98] Franklin worked with a number of other codes and ciphers in his international correspondence on behalf of the Continental Congress, and a number of examples of his coded correspondence have survived.[99]
34. Elbridge Gerry was a prominent radical in pre-Revolutionary Massachusetts, where he served as a member of local Committees of Correspondence and Committees of Safety. Once the Revolution started, he was elected to the Continental Congress, and served in the Constitutional Convention, and as Minister to France, Governor of Massachusetts, and Vice President of the United States.[100] Gerry was able to assist in deciphering the Benjamin Church correspondence early in the Revolution, and went on to have a distinguished career.[101]
35. Robert R. Livingston, Chancellor of New York, also served as Minister to France and Member of the Continental Congress, in which he served as Secretary of the Committee on Foreign Affairs.[102] One of Livingston's contributions to the Revolutionary cause was a 1700-part code that he designed for the Foreign Affairs Department in 1781.[103] The same code was used for private correspondence as well as government business.[104] Livingston sent George Washington a 1017-part code in 1782, while the Confederation government was still functioning and Livingston was head of the Department of Foreign Affairs.[105] While Livingston was in Paris on government business in 1802, Jefferson sent him a private letter and a cipher that could be used for their correspondence.[106]

36. Benjamin Tallmadge was George Washington's chief of military espionage for the region surrounding New York for much of the Revolution, during which he became an expert in using and breaking ciphered communications.[107] After rising to the rank of Lieutenant Colonel, he retired from military matters and was elected as a Member of Congress under the federal Constitution.[108]
37. James Lovell of Massachusetts was an orator, teacher, Member of the Continental Congress, and self-taught expert on matters of encryption and decryption.[109] He designed codes and ciphers for the Continental Congress and for use in private correspondence by members and their families.[110] David Kahn refers to Lovell as the "Father of American Cryptanalysis."[111] One of Lovell's codes was used by Madison and Randolph to replace a code that was compromised by a mail robbery.[112] Lovell was also employed to decipher the correspondence of Lord Cornwallis captured by General Nathaniel Greene's soldiers before the Yorktown campaign began in 1781.[113]
38. John and Henry Laurens were a father and son team from South Carolina. Henry, the father, was a merchant and planter who served as a Member of the Continental Congress and its President, after which he was appointed as a Peace Commissioner to negotiate the treaty of peace that ended the Revolution. John Laurens was an attorney, soldier, and envoy to France.[114] John Laurens used the codes supplied to him by Robert Livingston while he was in France.[115]
39. Silas Deane was an attorney and Member of the Continental Congress who served as a Commissioner to France. Some of his confidential correspondence with French officials was decoded by the British and "leaked" to the American Tory press, which deeply undercut his already controversial diplomatic career.[116] Examples of Deane's correspondence with John Jay, written in "invisible ink," are recorded.[117]
40. Numerous other examples of the use of ciphers and codes during and shortly after the Revolution could be provided,[118] but the materials cited so far should amply demonstrate that the Revolutionary era was a time of intense use of ciphers and codes by the Founders.

### C. Post-Revolution America and the Founders

41. After the adoption of the Constitution, and before the ratification of the Bill of Rights, codes, ciphers and other forms of secret communication were used by the Founders to speak freely only to those people they wanted to address. For example, in March 1789, after the Constitution was ratified and before the new President took office, George Washington corresponded with Henry Innes on the topic of the threatened secession of Kentucky from the newly-formed federal Union.[119] Washington promised to send Innes a "cypher" for their correspondence, and enjoined Innes to use it to cover their concerted efforts to defeat the secessionists. In the same correspondence, Washington looked forward with some reluctance to taking office as President, but regarded it as his duty to respond to the call of the citizens. Even as the acknowledged leader of the country, Washington still felt it appropriate to work with private citizens such as Innes to defeat the actions of a governing majority in Kentucky, and to use a cipher to support that political end.
42. George Washington and the Marquis de Lafayette, a French nobleman and Brigadier General of

the Continental Army under Washington, used a cipher for correspondence while LaFayette was in Paris in 1785.[120] Lafayette procured the cipher before leaving New York to return to France and sent the cipher to Washington, as well as taking it with him to France.[121] It should be noted that both LaFayette and Washington were private citizens in 1784-1785. In 1786, Reverend William Gordon made a gift of a cipher for correspondence to George Washington, a gift which Washington acknowledged with thanks.[122]

43. Another example from the period prior to the adoption of the Bill of Rights is compelling evidence of the importance of codes and ciphers to the Founders. While Jefferson was in Paris representing the new Republic, James Madison was a member of the House of Representatives. In the First Session of the First Congress, Madison introduced legislation that, when ratified by the states, became the Bill of Rights. The correspondence between Jefferson and Madison from the period covering the introduction and the Congressional debates over the Bill of Rights is partially enciphered.[123] It is revealing that Jefferson's August 28, 1789 letter to Madison in which he comments on the proposed First Amendment is partially enciphered, and that the comments about the text that became the First Amendment are contained in a paragraph immediately following a partially enciphered paragraph.[124]
44. Prior to the adoption of the Bill of Rights, Madison and Jefferson also used a 1700-word code for confidential discussion of sensitive personal and political issues. Professor Weber provides three examples from 1783, where Madison discusses his unsuccessful courtship of Catherine Floyd, personal political rivals, and the need to raise taxes.[125] It is therefore accurate to say that when, in 1791, "Americans adopted the Bill of Rights, communications were far more secure than they are today. Before the invention of the telephone, the radio, and the long-distance microphone, one could have a secure conversation by going for a quiet walk in an open field. Correspondents could encrypt letters in ciphers no government could break."[126] For over one hundred years, that statement remained substantially correct.

## IV. Extensive Private Use of Secret Communications Has Continued to the Present Day

### A. 1791 to 1800

45. From 1791 through the patenting of Samuel Morse's telegraph and beyond there has been widespread and common use of codes, ciphers, and other modes of secret communication. Perhaps the most compelling example of continued use of secret modes of communication is provided by the correspondence of James Madison and Thomas Jefferson during the administration of John Adams, who served as President from 1793 to 1801. A scholar who carefully studied and compiled the correspondence of Madison and Jefferson concluded that, in 1793, Jefferson and Madison were forced to resort to an earlier cipher.[127] "[T]he increasing hostility to the excesses of the French Revolution and the stresses and strains of organizing an opposition party forced Madison and Jefferson to be more circumspect about letters that they put into the public mail. ... By August [1793], they resorted to their 1785 cipher for encoding sensitive passages."[128]

46. There is evidence that Alexander Hamilton and his relatives and political associates used ciphers for secret communications at least between 1800 and 1803. On June 6, 1799, Hamilton's father-in-law General Philip Schuyler wrote to Hamilton promising to send him a "cypher" for their correspondence.[129] Hamilton wrote to Rufus King on January 5, 1800, conveying some information and indicating that he would wait for a cipher before communicating other information.[130] From New Orleans, in what eventually became Louisiana, on May 23, 1803, Hamilton was sent a cipher for correspondence and a very detailed set of instructions for its use--all in the French language.[131]
47. Aaron Burr, a former Vice President, sent a "political code" to Congressman Edward Livingston in 1806,[132] and Burr and his associates used secret, enciphered correspondence as part of their scheme to establish a new government in territory under the control of Spain.[133] Chief Justice Marshall accepted into evidence the "translated" (or decrypted) correspondence authored by Burr, allowing the recipient of the letters to act as a government fact witness and as the only decoder, even without the original letters in evidence.[134]
48. Before taking office as President in 1801, Jefferson invented one of the most sophisticated cipher devices of the Nineteenth Century. It was a "cipher cylinder," and has been described as "far ahead of its time," and as a device that "would have withstood any cryptographic attack of those days."[135] Professor Weber describes the cipher cylinder invented by Jefferson as a "brilliant mask" of "twentieth century security."[136] Professor Weber also gives a precise description of the specifications for the device and says that it was not surpassed until the U.S. Army conducted work to improve on it in the 1920s.[137] Professor Froomkin says that the Jefferson cylinder was still in use by the United States Navy in 1967.[138]
49. Jefferson's cylinder was a partial response to a broad need for secrecy. "In the years after 1780, Jefferson, James Madison, James Monroe, and a covey of other political leaders in the United States often wrote in code in order to protect their personal views on tense domestic issues confronting the American nation. Employing many codes and a few ciphers, they sought safety for their dispatches: they built security fences to protect their correspondence from political rivals and American postal officials."[139]

**B. Post-1800 Developments**

50. The need for secrecy and confidential communications has continued throughout American history. While it is beyond the scope of this paper to provide a comprehensive review of post-1800 cryptographic developments, it is important to note that the historical evidence is perfectly clear on two points. First, a strong private demand for encryption products continued throughout this period, and was met by a number of different methods and competing suppliers.[140] Second, until after 1960, there is no evidence that the federal government believed it should exercise its powers to restrict the use of encryption technology by private citizens.[141]
51. In 1805, *A Dictionary to Enable Any Two Persons to Maintain A Correspondence With a Secrecy Which is Impossible for Any Other Person to Discover* was published in Hartford, Connecticut. The unknown author listed words and syllables in alphabetical order, and suggested means for

concealing the meaning of correspondence using the dictionary.[142] Henry Clay, as Secretary of State, was sent a privately invented cipher in 1827, but there is no record of its use.[143] In 1829, James Swaim published a book for prisoners, advising them on the uses of coded speech to communicate through walls.[144] A textbook published in Nashville in 1832 included a chapter on cryptography, including the invention of a "zig-zag" cipher.[145] The newborn railroad industry was already interested in cryptography in 1833, judging by an article in the American Rail Road Journal from that year.[146]

52. Samuel Morse's telegraph invention in 1844 created substantial demand for codes and ciphers because the sender and the recipient could save money by abbreviating their messages.[147] Of course, another primary benefit of the use of the codes and ciphers promoted by Morse and his partners was secrecy.[148]
53. The Morse telegraph led to the publication of hundreds of code and ciphers, with instructions on how to vary their use to conceal the meaning of messages.[149] Extending on the telegraph, Alexander Graham Bell is crediting with having used "frequency division multiplexing" to send numerous telephone messages over one wire at the same time.[150]
54. Through the Civil War and later periods of American history, the extensive private use of encryption technology continued apace.[151] In 1996, it is difficult to say what portion of the national economy is dependent on encryption, but widespread commercial and private interests continued an extensive use of cryptography into the present decade.[152] The modern communications industry could not efficiently use the vast fiber optic networks without "time division multiplexing" and the complex coding mechanisms that permit packet switching of electronic mail and other data messaging services.[153] Bruce Schneier's *Applied Cryptography* text is full of examples from banking and other vital parts of the economy, ranging from consumer banking to encrypted electronic mail.[154] Pay cable television and satellite television offerings are encrypted, giving rise to an underground market in codes and descrambling devices.[155]

### C. Publication of Crytographic Knowledge

55. Americans have not been shy about teaching and writing about cryptography. In 1945, Joseph Galland published an extensive bibliography of printed materials dealing with the subject of cryptography.[156] His bibliography included ten American treatises on cryptography subjects published between 1872 and 1943.[157] The Galland bibliography also listed forty-four commercial encryption ciphers or codes published in the United States between 1832 and 1942.[158] From Edgar Allan Poe to Herbert Yardley and other prominent Americans, Galland cites forty-seven articles published in American magazines and periodicals on the subject of cryptography after 1840.[159] Schneier's *Applied Cryptography* lists 1653 separate cryptographic publications and articles as references, the vast majority of which have been published since 1950.[160]
56. All of this publication activity occurred while cryptography was used for legitimate commercial business operations and to support a variety of illegal purposes. These included gambling rackets,[161] conspiracies to steal resources from the federal government,[162] espionage,[163]

and smuggling.[164] Despite the widespread commercial and private use of encryption, and its use in criminal enterprise, there is no evidence of any effort to control publication or distribution of information about encryption, even in wartime. For example, in 1942, shortly after the beginning of the United States' involvement in World War II, Helen Fouché Gaines published *Elementary Cryptanalysis, A Study of Ciphers and their Solution.*[165] The author's declared aim was to explain in detail how to use codes and ciphers for confidentiality in business and military affairs.[166] There is no indication that the publication was considered an extraordinary event, even in the midst of war, or that Ms. Gaines intention to provide military and business institutions the same level of knowledge was problematic.

**D. Courts and Cryptography**

57. The courts have not treated those persons who have used encryption, ciphers, and codes with any presumption of illegality. On the civil side of the court system, the few reported cases involving encryption demonstrate a recognition that encrypted communications and ciphers play a valuable role in commerce, and that evidence regarding their operation and effects is therefore admissible in evidence through qualified witnesses.[167] In criminal cases, evidence that a defendant used a cipher or encryption has been allowed (as in *United States v. Burr)* as proof of the means used to commit an illegal act, but as proof of an illegal act by itself.[168]

**E. Patents for Cryptography**

58. It is also important to note that the United States Patent Office granted and published 105 patents on cryptological devices between 1874 and 1928.[169] Between 1928 and 1953, the same Office granted 133 such patents.[170] Important cryptological patents are still being granted in this decade.[171]
59. In 1977, a patent application in the field of cryptography and a patent for a telephone scrambling device were preliminarily classified as secret under the Inventions Secrecy Act.[172] The encryption patent application involved advanced mathematical techniques for encryption, and caused concern to the National Security Agency, which eventually reversed its position and declassified both patent applications.[173] The Inventions Secrecy Act authorizes the Commissioner of Patents to refuse to issue patent secrecy orders, but it has not been effective in preventing the public dissemination of a number of strong, unpatented encryption products, and is not a mainstay of federal attempts to control encryption.[174]

**F. Post World War II Developments**

60. After World War II, the advent of rapid computing devices gave the government and private industry the ability to use very sophisticated methods of encryption to ensure reliability and secrecy of communications. Commercial uses continued, and the computer software industry that became such a large part of the American economy took over the traditional role of the old cipher

and code-publishing companies that had flourished in the Nineteenth and Twentieth Centuries.[175]

61. A recent National Research Council report describes the state of encryption in the United States today in terms of strong demand and multiple domestic and international vendors.[176] Encryption is widely used to safeguard information in networked computer systems, to protect privacy, to ensure the integrity and confidentiality of records, files, and electronic mail, to secure facsimile transmissions against intrusion, and to discourage industrial espionage.[177] Privacy and integrity--and confidence in the ability of the communications networks to provide those qualities--have been greatly enhanced and made available on a ubiquitous basis as a result of the wide distribution of computing power and information processing technology.[178] Encryption plays a significant role in ensuring acceptable levels of privacy and integrity in communications.[179]
62. Before the wide distribution of personal computers led to widespread demand for encryption software for individual use, the federal defense and intelligence communities spent unknown (but massive) amounts of resources to obtain encryption technological superiority over the world.[180] After World War II, the National Security Agency and other agencies, including the Federal Bureau of Investigation, developed an extraordinary capacity to decrypt the communications of the foreign and domestic opponents of the United States.[181] For the first time in American history, massive federal investments in computing power gave the government an unquestioned encryption superiority over foreign diplomats and Americans. The ability to break codes and ciphers no longer depended on the brilliant intuitions of a few experts, but was driven by the power of the federal agencies to engage massively parallel computing to attack any cipher, and to break it in hours.[182]

### G. The Government Acts to Control Encryption

63. In 1977, with the support of the National Security Agency (NSA), the National Bureau of Standards certified for commercial use an IBM-developed encryption chip known as DES (or the Data Encryption Standard).[183] The National Security Agency "guaranteed" that the DES would be a secure system for commercial users.[184] By 1987, the NSA had decided that it would no longer guarantee the security of the DES product[185] and developed a policy of opposition to private cryptographic research, development and use as threats to government codes and intelligence gathering.[186] The DES product released to the public in 1977 was only a 56-bit key, while IBM had earlier developed and demonstrated a key of over 100 bits.[187] NSA argued that its efforts to restrict knowledge about and access to advanced encryption were based on policies of denying knowledge for the public's own good, on economic efficiencies, and a need for uniformity in computer information security.[188] Despite these arguments, neither the NSA nor the National Bureau of Standards (later known as the National Institute of Standards and Technology or NIST) were given statutory authority over encryption standards in the private sector.[189] Although the NSA convinced President Reagan to sign National Security Decision Directive 145,[190] an Executive Order that seemed to give NSA authority over all private sector information that could affect national security, that Directive was withdrawn in 1987.[191]

64. DES quickly became an international standard for cryptography.[192] It was of such widespread use and of such venerable age that, by 1993, the 56-bit key was subject to being compromised in relatively short periods of time (less than four hours) by anyone who could command enough computing power.[193] The government deemed this an opportune moment to launch its campaign for adoption of a new government-provided encryption product--the ill-fated Clipper Chip.[194] This proposal, under which the government would have served as its own "escrow" agent for the keys to encryption used by virtually any private citizen, was a failure because the Clipper Chip was cryptologically flawed.[195] Although the Clipper Chip may have progeny, its initial generation was rejected.
65. By the early 1990s, the balance of encryption technology had effectively shifted back to the citizen who was able to invest in readily available software products.[196] "With ever more secure methods of encryption becoming easier to use, U.S. residents can protect their electronic communications and records so well that they are able to frustrate interception attempts by even the most sophisticated government agencies."[197] The government has responded on at least three fronts.[198] First, the Clinton Administration pushed through Congress a law requiring every substantial telecommunications carrier in the United States to modify its network to assist federal agencies in installing and maintaining wiretaps.[199] Second, the Clipper Chip proposal was brought forward.[200] Third, the government has continued a very aggressive program of enforcement of the munitions export regulations (known as ITAR) against advanced encryption software products.[201] Because the practical effect of the ITAR enforcement scheme is to deny U.S. businesses a chance to compete in the bustling international market for strong encryption products,[202] it can easily be surmised that the real purpose of the ITAR enforcement scheme is to restrict and discourage domestic development of encryption technology that is stronger than that which the government wishes U.S. citizens to possess and use.[203]
66. The coordinated efforts of the intelligence and law enforcement agencies throughout the last ten years demonstrate a very strong intention by those agencies to maintain their relatively recently-achieved technological superiority over the citizenry. Professor Froomkin concluded that the government "makes no secret of its hope that the combination of federal standard-setting, federal purchasing power, and fine-tuning of export control will allow it to impose a de facto standard on the public."[204]

## V. Any Attempt to Abolish or to Substantially Burden the Liberty of Secret Communication Should Meet a Strong Presumption of Unconstitutionality

67. Throughout the history of the American Republic, the citizens have been able to speak freely and confidentially on topics, and to the audience, of their choosing. In the last thirty to forty years the balance shifted in favor of the government eavesdropper. However, for many people, modern encryption technology has created an environment in which private or governmental actors who wish to invade and compromise the privacy and confidentiality of communications can only do so at great cost in time and computer facilities.[205] As has been discussed above, this is the situation

that existed for the great bulk of American history.[206] Given widespread domestic and international availability of strong encryption,[207] it would appear that nothing short of a drastic prohibition of strong encryption could restore the government's advantage in this area.

68. Federal law enforcement agencies have serious arguments to make in regard to terrorists, kidnappers, drug dealers, and child pornographers, as examples of the types of criminals who misuse encryption.[208] The Clinton Administration has recently announced that it will centralize responsibility for encryption policy in a cabinet officer--the Secretary of Commerce--and that it will attempt to enlist other countries to impose encryption export controls on their economies.[209] It must be assumed that, where the stakes are so high, the government will at least consider banning the domestic use of strong, unlicensed encryption products.[210]

**A. What is the Difference Between 1796 and 1996?**

69. The Founders would not have accepted a government attempt to ban the use of ciphers and codes that were too strong for the government's convenience. Is 1996 materially different from 1796? What *is* different between 1796 and 1996 is the widespread availability of computers, strong encryption software, and long-distance telecommunications. It is as if Jefferson's cipher wheel has been electronically enabled, and the manual operation of the device has been automated. What effect should this have on the legal arguments? For purposes of analysis of the Constitutional issues, it may also be useful to assume that Jefferson's cipher wheel would be practically impossible for the government to defeat without a major commitment of computer resources. Even with this assumption, it is simply implausible to assume that the Founders would have accepted a prohibition on Jefferson's cipher wheel, for a variety of reasons.
70. By protecting his communications and raising a shield of privacy around his intentions and statements, Jefferson protected himself against the government and private interlopers. Relative to the government's abilities in 1796 (which were comparatively weak) Jefferson was able to maintain control over the message and the audience. It is simply implausible to suggest that Jefferson, Madison, Washington, Adams, Monroe *et al*. would have been willing to surrender the protection against government that ciphers provided, *because* the government found it expensive or impossible to crack the codes. Frustration of government intrusion was a major purpose of the Founders in using encryption, and that purpose would be utterly frustrated by government pre-selection of encryption.
71. It may be argued that adding speed and reliability to secret communications will change the fundamental nature of the practice, or make it more subject to abuse. This is not a sensible argument, given the history set out in this paper. Widespread availability of reliable and rapid, secret communication will not make the citizens more or less trustworthy than they were in 1791, or make the government better or worse than it was in the same year. It must be conceded that communications encryption, with speed and reliability, will mean that the government will be able to decipher a smaller percentage of messages with the same resources. This is not a radical alteration of the circumstances prevailing when the Bill of Rights was adopted in 1791. Thus, there is no material difference in regard to the balance of power between the citizens and their government in 1796 versus 1996; the citizens can have the upper hand if they choose to use an

excellent cipher.

72. International smugglers, pornographers, narcotic drug cartels, kidnappers, terrorists, and traitors will continue to use secret, illegal communications devices and encryption. By and large, international criminal enterprises are willing to pay the extra price for communications secrecy, and there does not seem to be the slightest evidence that the criminal community will restrict its purchases to the United States market.[211] The argument that the government can protect the United States by preventing the domestic deployment of strong encryption rests on several fallacies. First, it assumes that Americans have given the power to the government to decide in advance what technologies and modes of communication will be permitted. Second, it assumes that stunting U.S-based encryption development will protect the nation from international criminals, who, by definition are not concerned with domestic laws and regulations. Third, it assumes that the convenience and efficiency of the Executive Branch in law enforcement and intelligence should outweigh the liberty interests of private citizens, despite the historic practices and customs of the citizens.
73. These assumptions allow the Executive Branch to weigh its own convenience and needs against those of the citizenry.[212] The Constitution requires far more than administrative convenience as a rationale for displacement of a long-standing right.

## VI. Secrecy of Communications Serves Core Constitutional Interests and Should Be Protected as An Ancient Liberty

74. A mode of expression identified as an Ancient Liberty under the Constitution, encryption may find its textual support in a number of Constitutional provisions. A scheme of regulation under which Americans were required to use only those forms of encryption that were pre-approved by the government might run afoul of a number of constitutional provisions and rules. These would include the First Amendment,[213] the Fourth Amendment,[214] the Fifth Amendment,[215] and the Right to Privacy derived from the First, Third, Fourth, Fifth, Ninth and Fourteenth Amendments.[216] There is also a possible argument under the Thirteenth Amendment.[217] and the Postal Power granted to Congress in Article 1 Section 8 of the Constitution.[218]
75. All of those arguments are beyond the scope of this paper. However, as a demonstration of the potential relevance of some of the historical materials collected in this paper, this section will summarize the vital interests of the Founding generation that were protected by encryption technology. It is true to say that "in the early Republic, a well-constructed code could make private letters secure from political enemies, foreign foes, and highway robbers in America,"[219] but more should be said about the interests potentially protected by use of encryption.

### A. Protection of Dissent

76. It may be difficult for late Twentieth Century Americans to view George Washington, John Adams, and Thomas Jefferson as dissident voices seeking the protection of secret communications. The historic facts discussed above show that they and their fellow rebels against

the Crown sought refuge in encryption to enable political and social dissent. This need continued after the Treaty of Paris in 1783, however, because Congress had already instituted a system for government inspection and opening of the mails.[220] "Even though the mail to and from Congressmen continued to be legally sacrosanct, these [Congressional] resolutions [regarding mail surveillance] brought an atmosphere of suspicion in which secret codes and ciphers would thrive."[221]

**B. Protection of Freedom of Thought and Developing Ideas**

77. Perhaps the most compelling demonstration of the protection provided by encryption to freedom of thought and developing ideas (those not yet ready for the public eye) is the use made by George Washington and Henry Innes in opposing the Kentucky Resolves.[222] As a private citizen, Washington wanted to act privately and confidentially to instruct and assist Innes in his efforts to undermine the majority in the Kentucky legislature, and he did not want the glare of publicity to surround his correspondence with Innes. Numerous other examples of the protection afforded to developing opinions could be suggested.[223]

**C. Protection of Political Expression and Parties**

78. The protection afforded to political expression and parties is amply demonstrated by the ciphered correspondence between Jefferson and Madison during the Adams administration, as they sought to build an opposition party. Although they relied on the mail service provided by the government, they used encryption technology to hide from that same government their plans, intentions, and political moves.[224] They acted under a cloak of encryption in the same era when political dissent was punished by accusations of sedition, and when federal judges instructed juries that criticism of the federal government was sedition.[225] The emergence of the Republican party in the 1800 federal elections, with Jefferson as its Presidential candidate, owes much to the planning and secret correspondence permitted by ciphers that the government of the time could not conveniently break.

**D. Protection of Personal Privacy**

79. The Founders used secret communications methods to deny information to those not intended to receive it and to act as a "secure seal."[226] Abigail Adams summed it up neatly when she said that there were certain personal topics that she could not address in correspondence with her husband because of the lack of a cipher at a time when John Adams was in Paris.[227] Jefferson, Madison and others used ciphers to protect information about their romantic intentions.[228] Randolph corresponded with Madison about the painful topic of his wife's cancer.[229] Aaron Burr used a cipher to correspond with his daughter after his acquittal on treason charges, seeking to protect himself and his daughter from further governmental inspection.[230] Personal life suffered without secure communications.

## VII. Conclusion

80. "Because of foreign and domestic threats to liberty and freedom, codes and ciphers became integral elements in American public and private communication."[231] This summation of early American history shows that Americans have long enjoyed the ancient liberty of the use of ciphers, codes and other forms of secret writing. The federal government has, for only two generations, enjoyed the ability to quickly override consumer use of cryptography through powerful decryption technology. The government's superior decryption capacity is threatened (or perhaps it has practically evaporated) when average citizens can and do encrypt their communications and their records using powerful encryption products.
81. Absent abandonment of current government policy, the courts will inevitably be called upon to judge the balance between the government's asserted powers and the Ancient Liberty of secret communication.[232] Technological development should not have the effect of making Americans less free than the Founders. When the courts do eventually confront the issue, it is hoped that the judges do so with full knowledge of the technological and legal history of encrypted communications, and will recognize and uphold this Ancient Liberty.

---

# Footnotes

[*] Copyright, 1997, John A. Fraser, III. J.D., Washington & Lee Univ. School of Law, 1980; Candidate for LL.M. Degree, University of Virginia, 1997.

[1] See Lawrence Lessig, *The Path of Cyberlaw*, 104 YALE L.J. 1743, 1749-50 (1995) for a discussion of why encryption technology can restore vital privacy to personal communications.

[2] A "code" is a pre-arranged set of meanings assigned to particular symbols. A "cipher" is a means to disguise or "encrypt" a text regardless of its correspondence to a pre-arranged set of meanings. "Cryptography" includes the use and design of means to communicate messages so that only certain people can understand the intended message. "Cryptology" is the study of cryptography and cryptanalysis. *See* A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 713-14 (1995). Professor Froomkin's valuable article also includes a technical appendix that describes and defines a number of important cryptological concepts, *see id.* at 885-897.

[3] This paper does not deal with the export of codes, encryption algorithms, cipher devices, or encryption technology. *See Karn v. Dep't of State*, 925 F.Supp. 1 (D.D.C. 1996) *remanded for consideration under new Executive Order, per curiam*, No. 96-5121 WL 71750 (D.C. Cir. January 21, 1997) (export controls unreviewable); *Bernstein v. Dep't of*

*State*, 945 F. Supp. 1279 (N.D. Cal. 1996) (export controls on encryption software regulate speech and may be subject to review). Nor is the paper intended to address the technical and broad social contexts in which secrecy of communications may be desired by users. *See generally*, Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, ch. 1 (2d ed. 1996) (providing extensive definitions and examples of use); Stewart A. Baker, *Government Regulation of Encryption Technology: Frequently Asked Questions*, 452 PLI/Pat. 287 (1996) (overview of encryption by former General Counsel of National Security Agency). For an overview of communications privacy issues, see Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?* 44 Fed. COMM. L.J. 195 (1992).

[4] A number of authors have addressed a variety of sources of legal protection for secret modes of communications. The most helpful articles that address encryption issues include Renae Angeroth Franks, *The National Security Agency and its Interference with Private Sector Computer Security*, 72 IOWA L. REV. 1015 (1987); Dorothy E. Denning, *Edited Comments Concerning Regulating State Access to Encrypted Communications*, 1994 ANN. SURV. AM. L. 415 (1994); Timothy B. Lennon, *The Fourth Amendment's Prohibitions on Encryption Limitation: Will 1995 be like 1984?* 58 ALB. L. REV. 467 (1994); Mark I. Koffsky, Comment, *Choppy Waters in the Surveillance Data Stream: The Clipper Scheme and the Particularity Clause*, 9 HIGH TECH. L.J. 131 (1994); Martin E. Hellman, *Implications of Encryption Policy on the National Information Infrastructure*, 11 COMPUTER LAW. 28 (1994); Charles L. Evans, *U.S. Export Control of Encryption Software: Efforts to Protect National Security Threaten the U.S. Software Industry's Ability to Compete in Foreign Markets*, 19 N.C. J. INT'L L. & COM. REG. 469 (1994); Kristine M. Nelson, *The Clipper Initiative: Fact or Fiction in Future Encryption Policy*, 16 HAMLINE J. PUB. L. & POL'Y 291 (1994); Curtis E. A. Karnow, *The Encrypted Self: Fleshing Out the Rights of Electronic Personalities*, 13 J. MARSHALL J. COMPUTER & INFO. L. 1 (1994); Henry R. King, Note, *Big Brother, The Holding Company: A Review of Key Escrow Encryption Technology*, 21 RUTGERS COMPUTER & TECH. L.J. 224 (1995); Kirsten Scheurer, Note, *The Clipper Chip: Cryptography Technology and the Constitution--the Government's Answer to Encryption "Chips" Away at Constitutional Rights*, 21 RUTGERS COMPUTER & TECH. L.J. 263 (1995); Christopher E. Torkelson, *The Clipper Chip: How Key Escrow Threatens to Undermine the Fourth Amendment*, 25 SETON HALL L. REV. 1142 (1995); A. Michael Froomkin, *The Metaphor is the Key, Cryptography, The Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709 (1995); Phillip E. Reiman, *Cryptography and the Right to Be Unheard*, 14 J. MARSHALL J. COMPUTER & INFO. L. 325 (1995); and Jill M. Ryan, *Freedom to Speak Unintelligibly: The First Amendment Implications of Government-Controlled Encryption*, 4 WM. & MARY BILL RTS. J. 1165 (1996). Several authors have implied that the Founders could not have anticipated the development of relatively strong encryption technology. *See* Reiman *supra*, at 327 n.15 (1995) (First Amendment law does not "fit" cryptography); M. Christina Ramirez, *The Balance of Interests Between National Security Controls and First Amendment Interests in Academic Freedom*, 13 J.C. & U.L. 179, 206 (1986) (uses of encryption have been almost exclusively military and

government); *cf.* Froomkin, *supra*, at 798 & n.372 (suggests that at the time of the Revolution, government was unable to break many private ciphers, and that the Founders enjoyed freedom in use of encryption). The assumption that the Founders did not anticipate encryption that is strong enough to defeat government surveillance, and constitutional protection against government attempts to control encryption, is incorrect in light of the history of ciphers, codes, and secret writing in the early days of the Republic.

[5] "In some times and places the even more capacious new media will open wider the floodgates for discourse, but in other times and places, in fear of that flood, attempts will be made to shut the gates." Ithiel de Sola Pool, *Technologies of Freedom* 250 (1983).

[6] It is not within the scope of this paper to describe the process of selective incorporation that the Supreme Court has followed. A brief summation of the doctrine of incorporation may be found in *The Oxford Companion to the Supreme Court of the United States* 426-27 (Kermit L. Hall *et al.* eds., 1992).

[7] H*ague v. Comm. for Indus. Org.*, 307 U.S. 496 (1939).

[8] *Id.*

[9] *United States v. Grace*, 461 U.S. 171 (1983) (striking down federal ban on leaflet distribution outside the Supreme Court itself); *Schneider v. Irvington*, 308 U.S. 147 (1939) (invalidating ordinances that barred public distribution of leaflets).

[10] *Martin v. Struthers*, 319 U.S. 141 (1943) (ordinance that forbids door-to-door distribution of literature is invalid as applied to Jehovah's Witness).

[11] *Carey v. Brown*, 447 U.S. 455 (1980) (statute that prohibited residential picketing was unconstitutional).

[12] *Hurley v. Irish-American Gay, Lesbian and Bisexual Group of Boston*, 115 S.Ct. 2338 (1995).

[13] *NAACP v. Claiborne Hardware*, 458 U.S. 886 (1982) (consumer boycott is form of protected expression).

[14] *New York Times v. Sullivan*, 376 U.S. 254 (1964).

[15] *Hustler Magazine v. Falwell*, 485 U.S. 46 (1988).

[16] *City of Ladue v. Gilleo*, 512 U.S. 43 (1994).

[17] *Meyer v. Nebraska*, 262 U.S. 390 (1923). Over a lone dissent by Justice Holmes, who thought that preventing the emergence of towns dominated by foreigners was a strong state interest, the majority overturned a Nebraska law that criminalized the teaching of German to school-age children. *Accord Farrington v. Tokushige*, 273 U.S. 284, 298-99 (1927) (overturning Hawaiian language restriction in schools); *Bartels v. Iowa*, 262 U.S. 404 (1923) (prohibition on teaching foreign languages is unconstitutional); *Yu Cong Eng v. Trinidad*, 271 U.S. 500 (1926) (statute prohibiting use of some languages in business records is unconstitutional). *See also Spence v. Washington*, 418 U.S. 405, 411 n.4 (1974) (statute that restricts content of speech is unconstitutional even though it permitted other words to be used). *Cf. United States v. Bromley*, 53 U.S. 88 (1851) (implicitly recognizing First Amendment right to carry messages, but upholding mail monopoly law).

[18] 514 U.S. 334 (1995). The *McIntyre* case is analyzed in Lee Tien, *Who's Afraid of Anonymous Speech? McIntyre and the Internet*, 75 OR. L. REV. 117 (1996); Richard K. Norton, *McIntyre v. Ohio Elections Commission: Defining the Right to Engage In Anonymous Political Speech*, 74 N.C. L. REV. 553 (1996); and Erika King, Comment, *Anonymous Campaign Literature and the First Amendment*, 21 N.C. CENT. L.J. 144 (1995).

[19] The factual description of the *McIntyre* case is taken from the majority opinion, 514 U.S. at 337-41.

[20] 514 U.S. at 338 n.3.

[21] 514 U.S. at 343 n.6. The anonymous authors included James Madison, Alexander Hamilton, and John Jay.

[22] 514 U.S. at 357.

[23] 514 U.S. at 358.

[24] 514 U.S. at 358. Justice Thomas has pursued a jurisprudence of original intent in matters of Constitutional law from his first days on the Supreme Court. For Justice Thomas, "the Constitution is a written instrument. As such its meaning does not alter. That which it meant when adopted, it means now." *South Carolina v. United States*, 199 U.S. 437, 448 (1905), quoted in the concurring opinion by Justice Thomas in *McIntyre*, 514 U.S. at 359.

[25] This is plainly stated in Part IV of Justice Thomas' concurring opinion, where he criticizes the majority for its deviation from the "original understanding" of the First

Amendment. 514 U.S. at 370.

[26] 514 U.S. at 359.

[27] 514 U.S. at 359, quoting from *Lynch v. Donnelly*, 465 U.S. 668, 673 (1984) (Establishment Clause case). Justice Thomas makes a point in his concurring opinion of citing cases in which a majority of the Court has rested its judgment on the original intent of the Framers. These cases include *INS v. Chadha*, 462 U.S. 919 (1983) (separation of powers and Congressional veto). 514 U.S. at 359.

[28] 514 U.S. at 360.

[29] There is a description of the John Peter Zenger seditious libel trial. 514 U.S. at 361.

[30] The actions and opinions of Elbridge Gerry, Henry Laurens, John Penn, and Merriweather Smith are quoted in describing the reactions of the Continental Congress to anonymous criticism in 1779. 514 U.S. at 361-62. The anonymous writings of William Livingston, governor of New Jersey, and the New Jersey legislature's reactions to anonymous attacks on it, are also described. 514 U.S. 362-63.

[31] 514 U.S. at 363-69.

[32] *Id.* at 367.

[33] *Id.*

[34] *Id.* at 368-69.

[35] *Id.* at 370.

[36] *Id.* Having found the original understanding, Justice Thomas holds that there is no need for further analysis of content-based speech restrictions developed in prior cases.

[37] *Id.* at 371.

[38] Justice Scalia quotes Thomas Jefferson, writing to Judge William Johnson in 1823, and criticizing Chief Justice John Marshall's actions in *Marbury v. Madison* :

> "[O]n every question of construction, [we should] carry ourselves back to the time when the Constitution was adopted; recollect the spirit manifested in the debates;

> and instead of trying [to find] what meaning may be squeezed out of the text, or invented against it, conform to the probable one in which it was passed."

514 U.S. at 372 (Scalia, J., dissenting) (quoting 15 *Writings of Thomas Jefferson* 439 , 449 (A.Lipscomb ed., 1904) (letter to William Johnson, June 12, 1823)).

[39] Justice Scalia characterizes the historical materials cited by Justice Thomas as "partisan claims in the debate on ratification" and said that the cited materials did not concern "the point before us." 514 U.S. at 374.

[40] Justice Scalia would have gone further to uphold the Ohio restriction, arguing that the "universal" and "long-established" legislative practice should be preferred over what he characterized as "historical and academic speculation." *Id.* at 377 n.3. Because the identity of a speaker is at the "periphery" of the First Amendment, Justice Scalia would allow later historical actions by the states to override the earlier historical evidence when the earlier history is not directly on point. *Id.* at 378.

[41] Regardless of the criticisms of this "original intent" jurisprudence, it should be observed that evidence regarding the intent of the Framers has been utilized in Supreme Court opinions since the earliest years of the Court. Chief Justice John Marshall asserted that *Marbury v. Madison*, 5 U.S. 137 (1803), was controlled by the original intent of the Founders. Justice Brennan relied on original intent in *School District of Abington Township v. Schempp*, 374 U.S. 203, 294 (1963) (concurring opinion), where he said, "[T]he line we must draw between the permissible and the impermissible is one which accords with history and faithfully reflects the understanding of the Founding Fathers." In a number of areas, the actions and opinions of Thomas Jefferson and James Madison carry great weight because of their influential role in the formation of the nation, the Constitution, and the Bill of Rights. *See, e.g., Graham v. John Deere Co.*, 383 U.S. 1 (1966) (patent law interpretation).

[42] *Clark v. Community for Creative Non-Violence*, 468 U.S. 288 (1984); *See United States v. O'Brien*, 391 U.S. 367 (1968) (symbolic speech and content-neutral, tailored restrictions).

[43] *Turner Broadcasting Sys. v. FCC*, 512 U.S. 622 (1994). The importance of the speech/conduct dichotomy can also be seen in *Bernstein v. Dep't of State*, 945 F. Supp. 1279 (N.D. Cal. 1996), where the district judge concluded that encrypted communications are a form of speech.

[44] *Compare City of Ladue v. Gilleo*, 512 U.S. 43 (1994) (residential signs) *or McIntyre*, 514 U.S. 334 (1995) (anonymous political speech) *with Los Angeles City Council v. Taxpayers for Vincent*, 466 U.S. 789 (1984) (upholding ban on campaign signs on public

property).

[45] Thus, in holding that consumer boycotts were an ancient practice protected by the Constitution, the Court did not have to convincingly explain how concerted refusal to do business with Claiborne Hardware was not "conduct" reached by the antitrust laws. *NAACP v. Claiborne Hardware,* 458 U.S. 886 (1982). However, in the same year, the Court held that concerted refusals by a union to load Russian grain ships ran afoul of U.S. labor laws prohibiting secondary boycotts, and that such conduct is not protected by the First Amendment. *Int'l Longshoreman's Ass'n v. Allied Int'l,* 456 U.S. 212 (1982). The distinction would appear to be that organized labor did not demonstrate any deep historic roots for its harbor boycott practices.

[46] Each of the forms of communication or expression that the Court has treated as an "Ancient Liberty" can be regulated to some extent when it is abused to inflict demonstrable, non-political harm on other persons. *See Organization for a Better Austin v. Keefe,* 402 U.S. 415 (1971) (overturning injunction against residential picketing, but reserving power to prevent abuses); *Int'l Bhd. of Elec. Workers v. NLRB,* 341 U.S. 694, 705 (1951) (picketing for unlawful purpose not protected).

[47] By using the term "forms or types of expression or communication," it is not meant that the mode or style of expression has been held protected without regard to context--the elements of expression other than the mode of expression. The Supreme Court has dealt with many types of regulation of expression, including attempts by governments to regulate every element of expression, and has judged each of them in context. The elements of expression regulated by governments have included the motive or intent of the speaker (*see, e.g., R.A.V. v. City of St. Paul,* 505 U.S. 377 (1992)); the effect on the audience (*see, e.g., Chaplinsky v. New Hampshire,* 315 U.S. 568 (1942)); the identity of the speaker (*see United States v. Nat'l Treasury Emp.Union,* 513 U.S. 454 (1995) (striking down *ex ante* ban on speech of federal employees); *McIntyre v. Ohio Elections Commission,* 514 U.S. 334 (1995); *Talley v. California,* 362 U.S. 60 (1960)); the content of the message (*see Meyer v. Nebraska,* 262 U.S. 390 (1923)); the identity of the recipients of the expression (*see FCC v. Pacifica Foundation,* 438 U.S. 726 (1978); *Sable Communications v. FCC,* 492 U.S. 115 (1989)); the quantity or volume of the expression (*see Buckley v. Valeo,* 424 U.S. 1 (1976); *Ward v. Rock Against Racism,* 491 U.S. 781 (1989)); the desire of the recipient to receive the materials (*see Lamont v. Postmaster General,* 381 U.S. 301 (1965)); and the means of delivery of the expression (*see City of Lakewood v. Plain Dealer Pub. Co.,* 486 U.S. 750 (1988) (newsracks); *City of Los Angeles v Preferred Communications, Inc.,* 476 U.S. 488 (1986) (cable television); *Miami Herald Pub. Co. v. Tornillo,* 418 U.S. 241 (1974) (newspaper)). A particular governmental regulation may impinge on one or more of the elements of expression, but there does not appear to be a separate rule governing any of the different elements. For example, a hypothetical regulation restricting the use of American Sign Language, widely used by speech-disabled persons, would impinge (at least) on the elements of identity, content, and audience. There does not appear

to be a separate line of cases for each element in this example, nor would there appear to be a rule for those types of regulation that impinge on numerous elements of a type of expression. The cases recognizing certain types of expression as having a historic and protected role in American history do not limit their holdings to any one element of expression or communication. Thus, in *Meyer v. Nebraska,* 262 U.S. 390 (1923), when the Supreme Court held that speaking and teaching a foreign language to a school-age child was protected, the holding necessarily dealt with the elements of the speaker, the audience, the content, and the means of delivery. The result is that there is no constitutional rule that protects all uses of a form or type of expression in all contexts. Context is critical. *See Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council Inc.,* 425 U.S. 748, 756 (1976) (First Amendment protects communication, its source, and recipients); *Griswold v. Connecticut,* 381 U.S. 479, 482 (1965) (First Amendment protects right to utter, to print, to distribute, to receive, to read, to inquire, to teach and to think).

However, the focus on context has not defeated the analytical efforts of the lower courts which have reviewed attempts to regulate use of minority languages. *See Yniguez v. Arizonans for Official English,* 69 F.3d 920 (9th Cir. 1995) (*en banc*), *rev'd on other grounds,* 117 S.Ct. 1055 (1997), (holding unconstitutional a requirement for use of English in transactions with state government); *Davenport v. City of Alexandria,* 710 F.2d 148, 150 n.3 (4th Cir. 1983) (*en banc*) (holding that a bagpipe performance is protected speech); *Bernstein v. Dep't of State*, 945 F. Supp. 1279 (N.D.Cal. 1996) (encrypted communications are protected speech); *Asian American Business Group v. City of Pomona,* 716 F. Supp. 1328 (C.D. Cal. 1989) (prohibition of completely non-English business signs violates First Amendment). *Cf. Cohen v. California,* 403 U.S. 15, 24 (1971) (Cohen had right to select offensive words to express his opposition to the military draft).

[48] A comprehensive review of the role played by historical precedents in all cases dealing with expression is outside the scope of this Article. There is no intention to imply that Constitutional protections for expression or communication are limited to those types of expression that meet this three-part test. Instead, it is asserted that the historical/legal approach evidenced in the Ancient Liberties line of cases does provide protection for some types of expression known and used by the Framers, with their evident approval. The Supreme Court has not limited its holdings to those subjects addressed by the Framers, and has extended First Amendment protection to prevent compelled speech (*Hurley v. Irish-American Gay, Lesbian and Bisexual Group of Boston,* 115 S.Ct. 2338 (1995)) and to protect association and speech through membership in unpopular groups (*NAACP v. Alabama ex. rel. Patterson,* 357 U.S. 449, 462 (1958). *See also United States v. United States District Court,* 407 U.S. 297, 314 (1972) (First Amendment protects right to speak confidentially).

[49] The discussion above includes, as examples, the use of political caricature and parody, consumer boycotts, picketing, anonymous political speech, and use of the streets and sidewalks for discussion of public issues. Abuses of these ancient liberties can be regulated,

but restrictions of the rights must be supported by a compelling demonstration of need, and must preserve the basic right. *See NLRB v. Gissell Packing Co.*, 395 U.S. 575, 616-20 (1969) (employer's speech to captive audience of employees is not protected speech where the understood meaning is one of intimidation or threat against exercise of protected right to organize); *United Broadcasting Co. v. FCC,* 565 F.2d 699 (D.C. Cir. 1977), *cert. denied*, 434 U.S. 1046 (1978) (renewal of broadcast license denied for radio station that persistently broadcast illegal lottery information in the form of coded scripture readings). A number of cases have dealt with abuses of the wearing of masks in public, with sometimes contradictory analyses. *Cf. Hernandez v. Commonwealth*, 406 S.E.2d 398, 401 (Va. App. 1991) (rejecting facial challenge to antimask law) *with Hernandez v. Superintendent*, 800 F.Supp. 1344, 1351 n.14 (E.D.Va. 1992), *app. dsm'd,* 8 F.3d 818 (4th Cir. 1993), *cert. denied,* 510 U.S. 1119 (1994) (challenger failed to show how antimask law infringed his freedom of association or freedom of speech). Froomkin, *supra* note 2, at 821-22 n.478 (1995) (collecting authorities on the mask issue.)

[50] David Shulman, *An Annotated Bibliography of Cryptography* (1976) [hereinafter Shulman, *Bibliography*].

[51] Shulman, *Bibliography*, *supra* note 50, at 3-26, included Giovanni Batista Porta, *Magiae Naturalis* 340-54 (1658) (describing the use of invisible inks); Johan Jacob Wacker, *De Secretis, Libri XVII* (1660) (ciphers); Sir Hugh Platt, *The Jewel House of Art and Nature* 13-15 (1593, 1613, and 1653) (use of secret ink and grille cipher device); John Willis, *The Art of Stenographie* (1602); 2 Francis Bacon, *The Two Bookes of Francis Bacon* 1.61 (1605) (describing use of ciphers); John Wilkins, *Mercury, or the Secret and Swift Messenger* (1641); Vandlus Hamid, *The Entire Art of Wryting in Secret* (1647); Noah Bridges, *Steganographie and Cryptographie* (1659); Sir Samuel Morland, *A New Method of Cryptography* (1666); John Falconer, *Cryptomenysis Patefacta; or the Art of Secret Information* (1685); Daniel DeFoe, *An Essay Upon Literature* 99-104, 109-10 (1726) (secret writing techniques); John Davys, *An Essay on the Art of Decyphering* (1737); and Philip Thicknesse, *A Treatise on the Art of Decyphering* (1772).

[52] John Wilkins was Bishop of Chester, Founder and First Secretary of the Royal Society, and Oliver Cromwell's Brother In-Law. David Kahn, *The Codebreakers* 155 (1967) [hereinafter Kahn, *The Codebreakers*].

[53] Wilkins, *supra* note 51, at ch. 2 (parables and scriptures); ch. 3 (inversion of known words); ch 4 (secret ink and paper); ch. 6 (changing the place of common letters); ch. 7 (keys); ch. 9 (double alphabets); ch. 11 (invented characters); ch. 12 (emblems and hieroglyphics); ch. 17 (sounds); ch. 18 (tunes and musical notes); ch. 20 (fire and smoke).

[54] Kahn, *The Codebreakers*, *supra* note 52, at 90 (Roger Bacon described use of ciphers in mid-1200s); 90-91 (Chaucer recorded instructions for astronomical device in cipher);

121-24 (Mary Queen of Scots' unsuccessful use of encryption to escape from prison in 1586-87). It appears that the need to communicate has always brought with it the need to communicate in confidence. For example, more than 5000 years ago in Sumeria and Iran, small symbolic figures representing articles of commerce were enclosed in clay envelopes that could only be read by being opened or broken. James Burke and Robert Ornstein, *The Axemaker's Gift* 42-44 (1995) (Sumeria); Denise Schmandt-Besserat, *Two Precursors of Writing: Plain and Complex Tokens, in The Origins of Writing* 34 (Wayne Senner ed., 1989) (Iran).

[55] Kahn, *The Codebreakers*, *supra* note 52, at 170-71.

[56] Kahn, *The Codebreakers*, *supra* note 52, at 171-74.

[57] Fletcher Pratt, *Secret & Urgent; the Story of Codes and Ciphers* 150-53 (1939).

[58] Harry Andrew White, *Those Human Puritans, in American Antiquarian Society Proceedings* 80-90 (1941).

[59] Fisher, George, *The American Instructor* 54-55 (1748) (printed by Benjamin Franklin and D. Hall).

[60] *See* James W. Thompson and Saul K. Padover, *Secret Diplomacy: Espionage and Cryptography, 1500-1815* (1963) [hereinafter *Secret Diplomacy*] (describing widespread European and British practice of opening private mails).

[61] 1 *The Papers of Thomas Jefferson* 15 (21 volumes) (Julian P. Boyd ed., Princeton, Princeton Univ. Press 1952-1983) [hereinafter *Jefferson Papers*].

[62] One of the earliest acts of the Continental Congress was to order that its Committee handling foreign correspondence use "cyphers." Ralph E. Weber, *Masked Dispatches: Cryptograms and Cryptology in American History*, 1775-1900 5-6 n.6. (1993) [hereinafter Weber, *Masked Dispatches*].

[63] David W. Gaddy, Introduction to Weber, *Masked Dispatches*, *supra* note 62.

[64] *Id.*

[65] Edmund Cody Burnett, *Ciphers of the Revolutionary Period*, 22 American Historical Review 329 (1917) [hereinafter Burnett, *Ciphers of Revolution*] "During the Revolutionary period cipher was employed extensively not only in public correspondence where secrecy was especially important but in the private correspondence of public men as well." *Id.*

[66] An excellent general overview of the use of a tremendous variety of ciphers and encryption devices during the Revolutionary era is contained in Burnett, *Ciphers of Revolution*, *supra* note 65. Another superb summary is Weber, *Masked Dispatches*, *supra* note 62, at 4-68. Professor Weber sums up the attitude of the Founders as follows: "At the time of the American Revolution, the American Founding Fathers did not believe codes and ciphers were employed for purposes of evil and cruelty. Rather, they viewed secret writing as an essential instrument for protecting critical information in wartime, as well as in peacetime." *Id.* at 4.

[67] Ralph E. Weber, *United States Diplomatic Codes and Ciphers, 1775-1938* 22-23 (1979) [hereinafter Weber, *United States Diplomatic Codes*]; Kahn, *The Codebreakers*, *supra* note 52, at 174-76.

[68] Kahn, *The Codebreakers*, *supra* note 52, at 176.

[69] G.J.A. O'Toole, *Honorable Treachery: A History of U.S. Intelligence, Espionage, and Covert Action from the American Revolution to the CIA* 36-49 (1991). Washington's detailed instructions on use of invisible ink are printed at 47.

[70] Kahn, *The Codebreakers*, *supra* note 52, at 176-77.

[71] Weber, *Masked Dispatches*, *supra* note 62, at 57-59; Kahn, *The Codebreakers*, *supra* note 52, at 177-80.

[72] Weber, *Masked Dispatches*, *supra* note 62, at 21-22.

[73] Correpondence between John Adams, Abigail Adams, and James Lovell, *in* 4 *The Adams Family Papers, Series II, Adams Family Correspondence* 162-63, 172-74, 253-54, 326-28 (L.H. Butterfield ed., 1973). [hereinafter *The Adams Papers*]. The editor's history and explanation of the Adams' uses of secret communications is in the appendix at *The Adams Papers*, *supra*, vol. 4, at 393-99. That history notes, among other things, that Lovell ciphers were also used by other Revolutionary War figures such as Benjamin Franklin, Horatio Gates, and W.F. Francis Dumas for private (i.e., non-governmental) correspondence in 1779-84. *The Adams Papers*, *supra*, vol. 4, at 394.

[74] *The Adams Papers*, *supra* note 73, vol. 4, at 326-28.

[75] *The Adams Papers*, *supra* note 73, vol. 4, at 393-94. When John Quincy Adams was United States Minister in Berlin in 1798, he devised a "sliding cipher" to protect his correspondence. Weber, *Masked Dispatches*, *supra* note 62, at 87-91.

[76] Jefferson's surviving correspondence, including those portions in code or cipher, is collected in *The Jefferson Papers*, *supra* note 61. As one of the more prolific users of secret communications methods, it should be understood that the following citations are merely examples. *The Jefferson Papers*, *supra* note 61, vol. 6, at 225-26; vol. 7, at 416-17, 444-46; vol. 8 at 580; vol. 12 at 102-03; vol. 15 at 153-54, 315-16, 366 (correspondence with Madison); vol. 6, at 233; vol. 7, at 290-91, 459-62, 563-64, 607, 638-40; vol. 8, at 42 (correspondence with Monroe); vol. 14, at 520-21; vol. 15, at 120, 188-90; vol. 16, at 6 (correspondence with Jay); vol. 8, at 173, 332-33, 394-95 (correspondence with Adams).

[77] Weber, *Masked Dispatches*, *supra* note 62, at 84-85.

[78] Weber, *United States Diplomatic Codes*, *supra* note 67, at 102-05, 382-401.

[79] Letters from James Madison to Philip Mazzei (July 7, 1781), *in* 3 *The Papers of James Madison*, at 176-81 (William T. Hutchinson & William M.E. Rachal eds., 1965) [hereinafter *The Madison Papers*] (refers to lack of cipher for letter to Mazzei); *supra*, vol. 2, at 211-16 & n.10 (partially encrypted letter from Mazzei dated November 30, 1780).

[80] *The Madison Papers*, *supra* note 79, vol. 3, at 293 & 294 n.6; vol. 4, at 174, 283-84. On May 28, 1782, Madison also corresponded with Joseph Jones, a member of the Continental Congress from Virginia, in an almost completely encrypted letter. *The Madison Papers*, *supra* note 79, vol. 4, 287-89.

[81] *The Madison Papers*, *supra* note 79, vol. 4, at 146-47, 148 n.9, 246-48, 350, 386-87, 396, 398 n.20, 418-19, 422 n.27, 435.

[82] *The Madison Papers*, *supra* note 79, vol. 4, at 262 (May 21, 1782 letter from Madison to Randolph, in which he says that he must decline to provide information to Randolph because the cipher is in use by Colonel Bland.)

[83] 10 *Dictionary of American Biography* 5-9 (Dumas Malone ed., 1933) [hereinafter *D.A.B.*]

[84] Weber, *United States Diplomatic Codes*, *supra* note 67, at 37.

[85] Weber, *Masked Dispatches*, *supra* note 62, at 53-54, 67.

[86] Weber, *Masked Dispatches*, *supra* note 62, at 58; Kahn, *The Codebreakers*, *supra* note 52, at 179.

[87] *D.A.B.*, *supra* note 83, vol. 8, at 330-31.

[88] Weber, *United States Diplomatic Codes*, *supra* note 67, at 93-97.

[89] *D.A.B.*, *supra* note 83, vol. 15, at 353-55.

[90] Weber, *Masked Dispatches*, *supra* note 62, at 22-23.

[91] *D.A.B.*, *supra* note 83, vol. 11, at 96-98. The City of London elected him Alderman as a show of disagreement with the government policy toward the American colonies after the fighting started in 1775. *Id.*

[92] Kahn, *The Codebreakers*, *supra* note 52, at 186.

[93] *D.A.B.*, *supra* note 83, vol. 11, at 96-98.

[94] *Secret Diplomacy*, *supra* note 60, at 177-79; s*ee also* James Raymond Wolfe, *Secret Writing: the Craft of the Cryptographer* 171 (1970) (describing A. Lee's unsuccessful effort to convince Continental Congress to use a "dictionary" code).

[95] *D.A.B.*, *supra* note 83, vol. 11, at 117-20.

[96] Weber, *United States Diplomatic Codes*, *supra* note 67, at 53, 56.

[97] 3 *Letters of Members of the Continental Congress* xxxiii (Edmund Cody Burnett ed., United States Gov't Printing Office, 1921).

[98] Kahn, *The Codebreakers*, *supra* note 52, at 185.

[99] Weber, *Masked Dispatches*, *supra* note 62, at 11-13.

[100] *D.A.B.*, *supra* note 83, vol. 7, at 222-227.

[101] Kahn, *The Codebreakers*, *supra* note 52, at 176.

[102] *D.A.B.*, *supra* note 83, vol. 11, at 320-25.

[103] Kahn, *The Codebreakers*, *supra* note 52, at 184.

[104] Weber, *Masked Dispatches*, *supra* note 62, at 83 describes use of this code by Jefferson and Madison for private affairs.

[105] Weber, *Masked Dispatches*, *supra* note 62, at 68.

[106] Weber, *Masked Dispatches*, *supra* note 62, at 77.

[107] Weber, *Masked Dispatches*, *supra* note 62, at 42-51; Kahn, *The Codebreakers*, *supra* note 52, at 177-79.

[108] *D.A.B.*, *supra* note 83, vol. 18, at 284-85.

[109] *D.A.B.*, *supra* note 83, vol. 11, at 438-39; Weber, *United States Diplomatic Codes*, *supra* note 67, at 27-35.

[110] Burnett, *Ciphers of Revolution*, *supra* note 65, at 331.

[111] Kahn, *The Codebreakers*, *supra* note 52, at 181.

[112] *Id.*

[113] Kahn, *The Codebreakers*, *supra* note 52, at 182. Lovell's other accomplishments are outlined at pages 183-84.

[114] *D.A.B.*, *supra* note 83, vol. 11, at 32-35.

[115] Weber, *Masked Dispatches*, *supra* note 62, at 67.

[116] *D.A.B.*, *supra* note 83, vol. 5, at 173-74.

[117] Shulman, *Bibliography*, *supra* note 50, at 3-8, describes the letters of Silas Deane to John Jay, June 11, June 18, September 17, and December 2, 1776.

[118] The prolific scholar, Edmund C. Burnett, who edited the *Letters of Members of the Continental Congress*, carefully noted the use of ciphers in a number of items of correspondence not otherwise noted above. These include vol. 3 at 231 & n.2 (May 12, 1778 letter from R.H.Lee to A.Lee, partially encrypted); vol. 4 at 155 (James Lovell to Horatio Gates, April 13, 1779, partially encrypted); vol. 4 at 424 & n.14 (June 1776 letter by Arthur Lee enclosing dictionary to be used as book cipher in correspondence by the Committee of Secret Correspondence); vol. 5 at 50 (James Lovell to B.Franklin, February

24, 1780, enclosing cipher); vol. 5 at 344 (Robert Livingston to Jay, August 26, 1780, enclosing cipher); vol. 8 at 19 (Monroe to Madison, February 1, 1785, partial encryption); vol. 8 at 421-22 (Monroe to Patrick Henry, August 12, 1786, alluding to a cipher); vol. 8 at 799 (Madison to Jefferson, September 21, 1788, partial encryption); vol. 8 at 812 (Madison to Jefferson, December 8, 1788, largely encrypted).

[119] *The Writings of George Washington*. (John C. Fitzpatrick ed., United States Government Printing Office, Washington, D.C. 1944) [hereinafter Fitzpatrick, ed., *Washington Writings*]. The March 2, 1789 correspondence between Innes and Washington is reproduced at vol. 30, 214-15. Henry (or Harry) Innes was a prominent attorney and Revolutionary War patriot in Virginia, as well as the first United States District Judge in Kentucky under the new Constitution. *D.A.B.*, *supra* note 83, vol. 9, at 485-86.

[120] 2 *The Papers of George Washington, Confederation Series* 550-51 (W.W. Abbott ed., University Press of Virginia 1992) (letter from Lafayette to Washington dated May 11, 1785, largely but not entirely in cipher).

[121] *Id.* at vol. 2, 226-28 (letter from Lafayette to Washington, December 21, 1784).

[122] Fitzpatrick, ed., *Washington Writings*, *supra* note 119, vol. 28, at 411-12.

[123] *The Madison Papers*, *supra* note 79, vol. 12, at 201-07 (Madison introduces Bill of Rights in House); vol. 12, at 185-86 (May 27, 1789 Madison letter to Jefferson, partially encrypted, in which Madison tells Jefferson that he intends to introduce a Bill of Rights in the House); vol. 12, at 360-65 (August 28, 1789 partially encrypted letter from Jefferson to Madison, in which Jefferson comments favorably on the proposed Bill of Rights).

[124] *The Madison Papers*, *supra* note 79, vol. 12, at 364-65. The partially encrypted information was a comment about Mirabeau, an important figure in the French Revolutionary Directorate.

[125] Weber, *Masked Dispatches*, *supra* note 62, at 83 & nn.2-4. Weber provides numerous other examples from the period between the end of the Revolutionary War and the commencement of the new, federal government under President Washington. *Id.* at 84 (Monroe, Adams, Jay, Jefferson, Madison).

[126] Froomkin, *supra* note 2, at 798 & n.372. Froomkin here refers to the existence of the Vigenere cipher and its status as an unbreakable cipher at the time of the Revolution, citing Kahn, *The Codebreakers*, *supra* note 52, at 214-21. Evidence as to which of the Founders used the Vigenere cipher was not found in researching this paper, but the point is entirely correct that government did not have the upper hand at the time the Bill of Rights was

adopted.

[127] *The Republic of Letters: The Correspondence Between Thomas Jefferson and James Madison*, 1776-1826. 3 vols. (James Morton Smith ed., W.W. Norton & Co., 1995). Mr. Smith notes the use of enciphered communications between Jefferson and Madison at vol. 2, p. 750.

[128] *Id.*

[129] *The Papers of Alexander Hamilton.* 27 vols. (Harold C. Syrett ed., Columbia University Press, New York, 1963-1987). The June 6, 1799 letter is found at vol. 23, 173.

[130] *Id.* at vol. 24, 167-69.

[131] *Id.* at vol. 26, 121-23. The editor includes the entire cipher and instructions, along with a translation.

[132] Weber, *Masked Dispatches*, *supra* note 62, at 93.

[133] The extraordinary case of *United States v. Burr*, 4 Cranch 455, 8 U.S. 455, 25 F.Cas. 2 (1807), presided over by Chief Justice John Marshall, contains a set of deciphered texts received by Brigadier General James Wilkinson in cipher, when Burr believed Wilkinson was part of his adventurous plot. 25 F.Cas. at 2-6. Marshall was familiar with ciphers from his diplomatic duties. Weber, *Masked Dispatches*, *supra* note 62, at 84.

[134] *United States v. Burr*, 4 Cranch 455, 8 U.S. 455, 25 F.Cas. 2 (1807) at 12 (opinion on commitment). The extraordinary political circumstances surrounding the charges of treason, the trial by a Chief Justice riding circuit, and the acquittal of Burr because of the weakness of the encryption evidence is described in Kahn, *The Codebreakers*, *supra* note 52, at 186-87. An extensive historical sketch concerning the case is also to be found at 25 F.Cas. 15.

[135] Kahn, *The Codebreakers*, *supra* note 52, at 192-95 (quotes from page 195).

[136] Weber, *Masked Dispatches*, *supra* note 62, at 6.

[137] Weber, *Masked Dispatches*, *supra* note 62, at 79-83. Weber also calls it "the most advanced cipher of its era." *Id*. at 83.

[138] Froomkin, *supra* note 2, at 798 & n.372.

[139] Weber, *Masked Dispatches*, *supra* note 62, at 6.

[140] Kahn, *The Codebreakers*, *supra* note 52, at 825-26, 836-53, provides information regarding the hundreds of commercial codes and commercially manufactured cipher machines sold in the United States.

[141] The statement holds for citizens, but during World War I and World War II, Presidents Wilson and Franklin Roosevelt issued Executive Orders or proclamations that severely restricted the ability of aliens to communicate in foreign languages by cable or telephone, and also prohibited the possession or use of ciphers and cipher codes by aliens. *See* J. Gregory Sidak, *War Liberty, and Enemy Aliens*, 67 N.Y.U. L. REV. 1402, 1413 n.57 (1992) (Wilson); Froomkin, *supra* note 2, at 851 & n.612 (Roosevelt).

[142] Kahn, *The Codebreakers*, *supra* note 52, at 192. The 1805 dictionary was followed by another, called the *Telegraphic Dictionary* (Brooklyn, NY 1812, Thomas Kirk, printer), cited in Shulman, *Bibliography*, *supra* note 50, at 3-9.

[143] Weber, *United States Diplomatic Codes*, *supra* note 67, at 191 & nn.50, 615.

[144] James Swaim, *The Mural Diagraph, or the Art of Conversing Through A Wall* (Philadelphia, 1829), cited in Shulman, *Bibliography*, *supra* note 50, at 1-33.

[145] William Thompson, *A New Method for Instruction of the Blind. Also a New Method of Cryptography, etc.* (Nashville, TN 1832), cited in Shulman, *Bibliography*, *supra* note 50, at 1-34.

[146] Anonymous, *Cryptography, or Methods of Secret Writing Described*, American Rail Road Journal n.p. (1833), cited in Shulman, *Bibliography*, *supra* note 50, at 1-34.

[147] Ithiel de Sola Pool, *Technologies of Freedom* 25-26 (1983). Kahn, *The Codebreakers*, *supra* note 52, at 189, says that Morse's telegraph "made cryptography what it is today."

[148] *See* Kahn, *The Codebreakers*, *supra* note 52, at 189, quoting Francis O.J. Smith, *The Secret Corresponding Vocabulary etc.*, (1845).

[149] *See, e.g.*, Henry J. Rogers, *The telegraph dictionary, and seamen's signal book, adapted to signals by flags or other semaphores; and arranged for secret correspondence, through Morse's electro-magnetic telegraph: for the use of commanders of vessels, merchants, &c.* (Baltimore, 1845), cited in Shulman, *Bibliography*, *supra* note 50, at 2-14.

[150] Pool, *Technologies of Freedom* at 37.

[151] Weber, *Masked Dispatches*, *supra* note 62, at 107-232; Kahn, *The Codebreakers*, *supra* note 52, at 214-853 (broad historic survey of Civil War to late 1960s). Because the focus of this paper is on the Revolutionary and immediate post-Revolution periods, this period will not be fully covered.

[152] Kahn, *The Codebreakers*, *supra* note 52, lists and documents use by smugglers (802-13), merchants hiding pricing codes from customers (824), for confidential financial information and business espionage (824-25), in oil and mining (825), in broadcasting (826), banking (826), telephony (826-27), fiber optic coding (829), signature authentication (829-30), pay-TV scrambling when approved by FCC (831-36), and dozens of other industrial uses (844).

[153] Pool, *Technologies of Freedom* at 37, 204.

[154] Schneier, *Applied Cryptography* at 139-47 (digital cash) 577-84 (electronic mail).

[155] *See* Pool, *Technologies of Freedom* at 178 (explaining cable and satellite television systems).

[156] Joseph Galland, *An Historical and Analytical Bibliography of the Literature of Cryptography*, (Northwestern Univ. Press, Evanston, Ill. 1945).

[157] In alphabetical order, Galland (pp. 21, 90, 94, 104, 108, 131, 172, 198, 200 and 206-07) cited George A. Bell, *Bell's Phonetic Cipher* ( Ohio State Journal, Columbus, 1881); Colonel Parker Hitt, *Manual for Solution of Military Ciphers*, (Press of the Army Service Schools, Ft. Leavenworth, Kansas1916); Frederick Edward Hulme, *Cryptography, or the History, Principles, and Practice of Cipher-Writing*, (London and New York, Ward, Lock & Co.1898); Edward Koch, *Cryptography; or Cipher Writing; a Study of Cryptography, etc*. (Belleville, Ill. Beuchler Pub. Co. 1936); Andre Langie, *Cryptography: A Study in Secret Writings* ( New York, E.P.Dutton & Co. 1922); Brig. Gen. Albert J. Myer, *A Manual of Signals: For the Use of Signal Officers in the Field, etc.* (New York, D. Van Nostrand 1872); Laurence Dwight Smith, *Cryptography, the Science of Secret Writing* (New York, W.W.Norton 1943); Elbert Wells, *Outdoor Signalling (* New York, Outing Pub. Co.1911); Maj. James A. White, *Military Signal Corps Manual* (New York, Wireless Press 1918); and Herbert O.Yardley, *The American Black Chamber* (Indianapolis, Bobbs Merrill Co.1931).

[158] Galland, *supra, passim.* The earliest commercial code noted by Galland was that of J.R. Parker, *The United States Telegraph Vocabulary, Being an Appendix to Elford's*

*Marine Telegraph Signal Book* (Boston, 1832).

[159] Galland, *supra, passim*. The articles by Edgar Allan Poe were published in *Graham's Magazine* (Philadelphia, 1841) in separate installments in July, August, October and December. Poe also wrote seriously about cryptographic subjects in some of his stories (*e.g., The Gold Bug*) and other articles cited by Galland at 145-46.

[160] Schneier, *Applied Cryptography* at 675-741.

[161] Kahn, *The Codebreakers, supra* note 52, at 818-21.

[162] Kahn, *The Codebreakers, supra* note 52, at 815-17 (describing use of decryption to break Teapot Dome scandal).

[163] *See Abel v. United States*, 362 U.S. 217 (1960) (use of cipher pads is evidence of espionage).

[164] Kahn, *The Codebreakers, supra* note 52, at 802-13. *See also* Froomkin, *supra* note 2, at 726-28 (describing criminal uses of encryption.)

[165] Helen Fouché Gaines, *Elementary Cryptanalysis, A Study of Ciphers and their Solution* (Boston, American Photographic Pub. Co. 1942).

[166] *Id.* at 2.

[167] *See, e.g., Home Box Office v. Gee Co Inc.*, 838 F.Supp. 436, 438 (E.D.Mo. 1993) (enforcing 47 U.S.C. Section 553(a)(1) ban on decryption of satellite signals without authorization); *Sylvester v. Ammons*, 101 N.W. 782, 784 (Iowa S.Ct. 1904) (lay expert can testify as to meaning of codes on merchant inventory); *W.L. Shepherd Lumber Co. v. Atlantic Coast Line R. Co.*, 112 So. 323, 327 (Ala. 1927) (expert may testify and decipher terms in an arcane shipping rate schedule); *Collender v. Dinsmore*, 55 N.Y. 200 (1873) (allowing parol evidence regarding meaning of shipping term "C.O.D." as between railroads). *Cf.* U.C.C. Section 1-201(39) ("signature" is sufficient if the symbol is intended as authorization); *Barber & Ross Co. v. Lifetime Doors, Inc.*, 810 F.2d 1276 (4th Cir. 1987) *cert. denied*, 484 U.S. 823 (1987) (trademark is sufficient signature when so intended). It is also interesting to note that the Supreme Court's listing of those types of speech or expression that can be prevented and punished without running afoul of the First Amendment has not included encrypted, coded, or secret expression. *See Chaplinsky v. New Hampshire*, 315 U.S. 568 (1942).

[168] *See, e.g., Abel v. United States*, 362 U.S. 217, 240-41 (1960) (cipher pads are

evidence of espionage); *Rice v. United States*, 35 F.2d. 689, 696 (2d Cir. 1929) *cert. denied*, 281 U.S. 730 (1930) (secret code used to authenticate telegrams in mail fraud case); *See also*, Kahn, *The Codebreakers*, *supra* note 52, at 802-15 (describing prosecution of smugglers during Prohibition based on expert testimony about use and interpretation of Acme commercial cipher).

[169] Shulman, *Bibliography*, *supra* note 50, at Part V, p.1 (listing patents).

[170] *Id.* at 2.

[171] Stewart A. Baker, *supra*, 452 PLI/Pat. at 308-310 (listing and describing patents granted in 1980-1995).

[172] 35 U.S.C. Sections 181-88 (1988).

[173] M. Christina Ramirez, *The Balance of Interests Between National Security Controls and First Amendment Interests in Academic Freedom*, 13 J.C.& U.L. 179, 204-05 (1986).

[174] Froomkin, *supra* note 2, at 751-52. It should also be noted that the "RSA" patent, United States Patent No. 4,405,829, issued in 1983 to Rivest, Shamir, and Adelman, is for a product that is stronger than the cryptography products that the government will permit to be exported.

[175] Kahn, *The Codebreakers*, *supra* note 52, at 850, describes the decline of the old code and cipher companies. Schneier, *Applied Cryptography* describes role of computers and software in modern encryption. Froomkin, *supra* note 2, at 719-726, 728-30 (describes numerous commercial uses for modern encryption software.)

[176] National Research Council, Cryptography's Role in Securing the Information Society, ch. 2 (May 30, 1996) [hereinafter *NRC Report*].

[177] Froomkin, *supra* note 2, at 718-26, 728-30; Note, 4 WM. & MARY BILL RTS. J. at 1171-73.

[178] *See* Joel Reidenberg and Francoise Gamel-Pot, *The Fundamental Role of Privacy and Confidence in the Network*, 30 WAKE FOREST L. REV. 105, 107-10 (1995).

[179] *Id.* at 109.

[180] Kahn *The Codebreakers*, *supra* note 52, at 672-733.

[181] *See generally*, James Bamford, *The Puzzle Palace* (Boston, Houghton, Mifflin, 1982) (history of National Security Agency).

[182] *See* Froomkin, *supra* note 2, at 738 (describing brute force technique for breaking cipher).

[183] Froomkin, *supra* note 2, at 736-37; Note, *The National Security Agency and Its Interference With Private Sector Computer Security*, 72 IOWA L. REV. 1015, 1016 n.8 (1987) [hereinafter *Iowa Note*]. Much of the same history of the Clipper Chip is provided in Torkelson, *supra*, 25 SETON HALL L. REV. at 1143-45. A significant, recent description of the government's efforts to use DES to control encryption knowledge and products is *NRC Report*, *supra* note 176, ch. 8, Recommendation 4.1.

[184] DES is a single key cipher, meaning that both sender and recipient use the same key to cipher and decipher the message. Froomkin, *supra* note 2, at 736: For the guarantee, *see Iowa Note*, *supra* note 183, at 1016 & n.10.

[185] *Iowa Note*, *supra* note 183, at 1017.

[186] *Iowa Note*, *supra* note 183, at 1017 & n.20.

[187] Froomkin, *supra* note 2, at 736-37 & n.110.

[188] *Iowa Note*, *supra* note 183, at 1024.

[189] *Iowa Note*, *supra* note 183, at 1027 & n.93.

[190] (September 17, 1984).

[191] *Iowa Note*, *supra* note 183, at 1032 & n.118.

[192] Froomkin, *supra* note 2, at 737-38; *NRC Report*, *supra* note 176, ch. 7, ch. 8, Recommendation 4.1.

[193] Froomkin, *supra* note 2, at 739-40.

[194] Froomkin, *supra* note 2, at 742-48.

[195] Torkelson, *supra*, 25 SETON HALL. L. REV. at 1166-69.

[196] The National Research Council, Section 2.4.2, concluded in 1996 that "[g]iven that various books, technical articles, and government standards on the subject of cryptography have been published widely over the past 20 years, the basic knowledge needed to design and implement cryptographic systems that can frustrate the best attempts of anyone (including government intelligence agencies) to penetrate them is available to government and nongovernment agencies and parties both here and abroad."

[197] Froomkin, *supra* note 2, at 716-17.

[198] This article does not deal with or interpret any of the bills introduced in Congress in recent times to address encryption issues.

[199] Communications Assistance for Law Enforcement Act, Pub.L.No. 103-414, 108 Stat. 4279 (1994).

[200] Torkelson, *supra*, 25 SETON HALL L. REV. at 1165-66.

[201] The International Traffic in Arms Regulations (ITAR), 22 C.F.R. Sections 120-130 (1996). The ITAR regulations are adopted under the authority of the Arms Export Control Act, 22 U.S.C. Sections 2751-2796d (1994). Under the ITAR enforcement scheme now in place, encryption products stronger than the DES standard approved by the government are routinely denied export permission. Froomkin, *supra* note 2, at 748-50; Torkelson, *supra*, 25 SETON HALL L. REV. at 1162-64.

[202] Torkelson, *supra*, 25 SETON HALL L. REV. at 1172 & n.161; Charles Evans, *U.S. Export Control of Encryption Software: Efforts to Protect National Security Threaten the U.S. Software Industry's Ability to Compete in Foreign Markets*, 19 N.C. J. INT'L L. & COM. REG. 469 (1994); Froomkin, *supra* note 2, at 750. In 1996, the National Research Council found that the effects of the ITAR enforcement policy had been to drive vendors of software to a "lowest common denominator" and to "distort" the global market. *NRC Report, supra* note 176, § 4.3.1. The NRC also found that "[t]he spread of cryptography is inevitable because in the information age the security of information will be as important in all countries as other attributes valued today, such as the reliability and ubiquity of information." *NRC Report, supra* note 176, § 8.1.2.3.

[203] The entire thrust of government policy on encryption is based on the assumption that it is reasonable and lawful to require that citizens communicate in a manner that is subject to government supervision and eavesdropping. The 1994 Communications Assistance to Law Enforcement Act reaches out to build this technological assumption into telephone networks. The Clipper Chip proposal had no more basic premise. The continued enforcement of ITAR against strong encryption products that are in computer readable

form, but not printed books, (*see Karn v. Dep't of State*, 925 F.Supp. 1 (D.D.C. 1996); *Bernstein v. Dep't of State*, 945 F. Supp. 1279 (N.D. Cal. 1996)) can also be seen as a further effort to carry out this philosophy, by discouraging domestic development and international distribution of encryption software not readily overborne by government computers. *See* Jill M. Ryan, *Freedom to Speak Unintelligibly: The First Amendment Implications of Government-Controlled Encryption*, 4 WM. & MARY BILL RTS. J. 1165, at 1174-89 (1996) [hereinafter *William & Mary Note*] (reviewing actions of federal government in recent years and concluding that goal is control of encryption).

[204] Froomkin, *supra* note 2, at 771.

[205] "[I]t is clear that the development and widespread deployment of cryptography that can be used to deny government access to information represents a challenge to the balance of power between the government and the individual. Historically, all governments under circumstances that further the common good, have asserted the right to compromise the privacy of individuals. ... [U]nbreakable cryptography for confidentiality provides the individual with the ability to frustrate assertions of that right." *NRC Report*, *supra* note 176, § 8.1.3.

[206] *Cf.* Froomkin, *supra* note 2, at 799-800 & n.375 (arguing that encryption may restore the "functional equivalent" of privacy of the 1790s, with the addition of rapid communications over great distances).

[207] The widespread, international availability of strong encryption is described in the National Research Council Report at ch. 8, Recommendation 4. *See also*, John Markoff, *2 Israelis Outline New Risk to Electronic Data Security*, N.Y. Times, October 19, 1996, at A38) (banking cards that use DES standard of encryption are vulnerable to flaws discovered by Israelis); Froomkin, *supra* note 2, at 738 (describing flaws in DES found by researchers and critics).

[208] *NRC Report*, *supra* note 176, §§ 3.2-3.3 (outlining law enforcement and signals intelligence needs of government).

[209] Organization for Economic Cooperation & Development (OECD), *OECD Meeting Makes Progress on Cryptography Guidelines* (visited December 13, 1996) <http://www.epic.org/events/crypto_paris/releaseE_OECD.html> (describing series of OECD meetings on development of global standards for cryptography and law enforcement access to encrypted information); Exec. Order No. 13,026, 15 C.F.R. 742.15, reprinted in 50 App. USCA §2403(6)

[210] John Mintz and John Schwartz, *Chipping Away at Privacy?* Washington Post, May 30, 1993 at H1 (describing plan to ban encryption not based on government escrow);

Professor Froomkin cites a speech where FBI Director Louis Freeh said that if all the FBI had was encrypted speech it was unable to decipher, then "the policy of relying on voluntary compliance with EES will have to change." Froomkin, *supra* note 2, at 810; *See William & Mary Note, supra* note 203, at 1188-89 (citing other testimony of federal officials).

[211] *See NRC Report, supra* note 176, § 3.2.4 (concluding, *inter alia*, that sophisticated and wealthy criminals such as drug cartel members have access to and use cryptography).

[212] The Executive Order signed on November 15, 1996 by President Clinton expressly states that it is not subject to judicial review, as did previous Executive Orders affecting encryption exports. *See Karn v. Dep't of State*, 925 F.Supp. 1 (D.D.C. 1996).

[213] Jaleen Nelson, *Sledge Hammers and Scalpels: The FBI Digital Wiretap Bill and its Effect on Free Flow of Information and Privacy*, 41 UCLA L. REV. 1139, 1162-67 (1994); Froomkin, *supra* note 2, at 811-822; *William & Mary Note, supra* note 203 at 1191-1221.

[214] Nelson, *supra*, 41 UCLA L. REV. at 1167-82; Froomkin, *supra* note 2, at 823-33; *See also* Randolph S. Sergent, *A Fourth Amendment Model for Computer Networks and Data Privacy*, 81 VA. L. REV. 1181 (1995).

[215] Froomkin, *supra* note 2, at 833-38; Greg S. Sergienko, *Self Incrimination and Cryptographic Keys*, 2 RICH. J.L. & TECH. 1 (1996).

[216] Froomkin, *supra* note 2, at 838-43.

[217] Arguably, one of the badges or incidents of peonage eliminated by the Thirteenth Amendment was control over all personal communications, including the refusal to allow any privacy in communications against the interests of the master. That this may be so can be seen from prisoner rights cases litigating the lack of any privacy in prison communications. Substantial elimination of communications privacy is a lawful aspect of status as a prisoner in a jail or penitentiary, and prison authorities do not violate the Constitution by imposing it on persons properly convicted and imprisoned. *See United States v. Van Poyck*, 77 F.3d 285, 290-91 (9th Cir. 1996) *cert. denied* , 117 S.Ct. 276 (1996) (approving routine taping of telephone calls with persons other than counsel); *Vester v. Rogers*, 795 F.2d 1179, 1183 (4th Cir. 1986) *cert. denied*, 482 U.S. 916 (1987) (routine censorship and absolute prohibition on inter-prison mail upheld); *Griffin-El v. MCI Telecommunications Corp.*, 835 F.Supp. 1114, 1122 (E.D. Mo. 1993) *aff'd*., 43 F.3d 1476 (8th Cir. 1994) (prisoner telephone conversations can be "branded" with introduction identifying origin of call despite prisoner's objections).

[218] *Ex Parte Jackson*, 96 U.S. 727, 733 (1877) held that the Fourth Amendment protected sealed letters placed in the United States Mail. Justice Field's opinion for the Court also held that, under the First Amendment, if "printed matter be excluded from the mails, its transportation in any other way cannot be forbidden by Congress."

[219] Weber, *United States Diplomatic Codes*, *supra* note 67, at 98.

[220] Weber, *United States Diplomatic Codes*, *supra* note 67, at 99-100, describes how Congress enacted mail opening legislation in 1782 and expanded and continued it in 1785 by a secret resolution, which was renewed in 1786.

[221] *Id.* at 100.

[222] *See supra* text accompanying note 119.

[223] For example, the Madison-Jefferson and Madison-Randolph correspondence is littered with use of encryption to protect developing thoughts on taxes (Weber, *Masked Dispatches*, *supra* note 62, at 83 & n.4 citing Madison to Jefferson, December 10, 1783) on personal political rivalries (Weber, *Masked Dispatches*, *supra* note 62, at 83 n.3, citing Madison to Jefferson, May 6, 1783) and Weber, *Masked Dispatches*, *supra* note 62, at 22-23 , citing Madison-Randolph correspondence. *See* discussion of Madison-Randolph political and personal correspondence at note 81, *supra*, and accompanying text.

[224] *See supra* text accompanying notes 127-128.

[225] Madison and Monroe found it necessary to use a private code while Monroe was in Congress. Weber, *United States Diplomatic Codes*, *supra* note 67, at 352-56, reproducing code.

[226] Weber, *United States Diplomatic Codes*, *supra* note 67, at 88. The same text reproduces surviving ciphers used for private correspondence by Madison and Randolph at 342-46.

[227] *See supra* text accompanying notes 74-75.

[228] The mails were subject to interception in America by robbers, and the carriers were sometimes stopped and searched. Weber, *United States Diplomatic Codes*, *supra* note 67, at 86, 97, 98.

[229] Weber, *United States Diplomatic Codes*, *supra* note 67, at 101.

[230] Weber, *Masked Dispatches*, *supra* note 62, at 95.

[231] Weber, *United States Diplomatic Codes*, *supra* note 67, at 107-08.

[232] Donald Merlin, *Origins of the Modern Mind* (1991), suggests that it is inevitable that humans will expand their reliance on coded communications. According to Merlin, the use of language is the "elemental component of human model building." (p. 219) Moreover, the human race has now launched itself, via the Internet and other external memory systems, on a third stage of evolution in which only those who know the "codes" can participate and access and use externally stored data. (p. 311-12) Because all forms of human communication can now be refined and expanded by digital devices, and because the modern mind is now a hybrid of internal and external memory, we are even more symbol and code-dependent than before. (p. 356, 382) A government that desires to control this process will feel compelled to control these essential communications pathways.