Encrypted Speech

Wanling Su* & Rahul Goravara**

29 STAN. TECH. L. REV. 58 (2026)

ABSTRACT

Text messaging has emerged as a defining medium of interaction for millions of Americans. This simple form of communication has transformed the way Americans advocate for change, share information, conduct business, and cultivate relationships. In response to growing security and privacy concerns, leading messaging platforms have begun encrypting text messages by default, igniting a debate over the scope of First Amendment coverage.

This Article challenges the notion that encrypted speech is a modern phenomenon requiring novel constitutional analysis. Drawing from extensive archival research into the private correspondence of America's foremost Founders, as well as doctors, lawyers, and businessmen of the era, this Article uncovers a forgotten yet vibrant tradition of encrypted communication. In response to an insecure postal system, eighteenth-century Americans routinely encrypted their politically, financially, and romantically sensitive letters using methods that proved impenetrable to surveillance efforts.

Encryption, it turns out, played an indispensable—and, fittingly, often overlooked—role in early American democracy. James Madison relied on encrypted correspondence to shield constitutional deliberations from public view, while Thomas Jefferson turned to anonymized and encrypted letters to organize the nation's first opposition party. This history demonstrates that encryption was not merely present but instrumental in forming the very constitutional protections now invoked by messaging platforms. As courts

---

* Assistant Professor, Indiana University Bloomington.

** Fellow, Georgetown University Law Center.

Thanks to the many colleagues who provided thoughtful feedback that helped refine this work, including Stephanie Barclay, Randy Barnett, Gabrielle Girgis, Jonathan Green, Margot Kaminski, Matthew Kugler, Paul Ohm, Robert Post, Bradley Rebeiro, Lawrence Solum, Abbey Stemler, Peter Swire, Blase Ur, and Felix Wu. Thanks also to participants at the Association of American Law Schools (AALS) New Voices in Civil Rights panel, the Eighth Junior Faculty Forum for Law and STEM at Northwestern Pritzker School of Law, and the Vincent and Elinor Ostrom Workshop Colloquium. Special thanks to Orin Kerr for his thought-provoking insights as a commentator. Mahishaa Balraj, Bohyoung Lee, and the staff of the *Stanford Technology Law Review* contributed outstanding editorial assistance. Joseph Ledford, Sophie Lin, Elizabeth Peppercorn, Ishani Sachdeva, Julia Stone, and Arielle Vertsman contributed helpful research assistance.

grapple with modern encryption technologies, this Article argues that they should recognize encrypted speech not as a novel challenge, but as the digital successor to a cherished Founding-era practice.

TABLE OF CONTENTS

I. INTRODUCTION

Millions of Americans are typing on smartphones with end-to-end encryption enabled.[1] Indeed, the most popular messaging application in America, iMessage, encrypts the text messages of unwitting iPhone users by default, giving them a greater degree of privacy and security than they perhaps realized.[2]

When text messages are encrypted end-to-end, only those communicating can read the messages.[3] The phone's manufacturer and the corporations that transmit the message across Wi-Fi networks and internet cables are intentionally left in the dark. To facilitate the messages' transmission across the internet, these third parties are given access to a scrambled conglomeration of characters that only the message's sender and recipient can decipher.

Encrypting a message is often described, by way of analogy, as writing a postcard in a foreign language that only the author and the intended recipient can understand.[4] Neither postal carriers nor criminals, domestic abusers, foreign despots, or law enforcement will be able to decipher the message if implemented correctly. While this technique ensures privacy, it also limits government access to Americans' communications,[5] igniting what many

---

[1] *Cf.* Jay P. Kesan & Rajiv C. Shah, *Setting Software Defaults: Perspective from Law, Computer Science and Behavioral Economics*, 82 NOTRE DAME L. REV. 583 (2006) (explaining that most people never change the default settings on their devices and applications).

[2] *See Messages & Privacy*, APPLE: PRIVACY POLICY (Sep. 15, 2025), https://www.apple.com/legal/privacy/data/en/messages [https://perma.cc/XQ72-JBJT]. ("We designed iMessage to use end-to-end encryption, so there's no way for Apple to decrypt the content of your conversations when they are in transit between devices.").

[3] *See* Andy Greenberg, *Hacker Lexicon: What Is End-to-End Encryption?*, WIRED (Nov. 25, 2014, 09:00 EST), https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption [https://perma.cc/842Y-EGNY].

[4] Regulating encryption, by analogy, would correspond to a legal requirement that individuals write their postcards in permitted languages that the government can translate. Accordingly, when one writes a postcard and places it in the mail, anyone handling the mail—including "hackers" who open the mailbox illegally—can translate what was written. *Cf.* Yniguez v. Arizonans for Off. Eng., 69 F.3d 920, 935 (9th Cir. 1995), *vacated on other grounds and remanded sub nom.* Arizonans for Off. Eng. v. Arizona, 520 U.S. 43 (1997) ("Language is by definition speech, and the regulation of any language is the regulation of speech.").

[5] The analogy fails, however, to capture the alternatives available to law enforcement. Although a tap on Wi-Fi networks or internet cables will not suffice if messages are encrypted, law enforcement can access the deciphered messages by seizing the recipient's smartphone or that of the sender. Attempts at mass surveillance, however, are undoubtedly impeded by encryption. For a discussion of Fifth Amendment issues raised by encryption, which are outside the scope of this Article, see generally Orin S. Kerr, *Decryption Originalism: The Lessons of* Burr, 134 HARV. L. REV. 905, 917 (2021) (analyzing Chief Justice Marshall's 1807 ruling in *United States v. Burr* on whether the Fifth Amendment privilege against self-

describe as "an extraordinary debate" among law enforcement, lawmakers, constitutional scholars, and technology leaders.[6]

Apple CEO Tim Cook has defended iMessage's encryption defaults against, at times, sharp criticism: "I don't want to read your texts . . . . This is not information that we need to know, that we want to know, that we should know."[7] He emphasized, "We think encryption is a must in today's world . . . . I wish it didn't have to be like that, but that is what it is," adding, "I don't know a way to protect people without encrypting."[8] When pressed, Cook argued that compelling companies to undermine end-to-end encryption would be "against the Constitution," a position he indicated Apple stands ready to defend in court.[9]

In contrast, Microsoft founder Bill Gates has expressed skepticism, arguing that "at the end of the day, we want a government that has visibility and we trust it to use that visibility on our behalf."[10] Gates doubts the constitutional merit of Apple's position, predicting that "over time . . . the government will decide not to be blind, and it will exercise its sovereign power not to be blind."[11]

Lawmakers have tried repeatedly over the past several years to rouse support for legislation requiring surveillance of text messages before they are encrypted. [12] In addition, the Department of Justice has issued public

---

incrimination protected Aaron Burr's secretary from being compelled to reveal the cipher to an encrypted letter).

[6] Lawrence Lessig, *The Path of Cyberlaw*, 104 YALE L.J. 1743, 1750 (1995).

[7] WALL ST. J., *Tim Cook Defends Apple's Encryption Policy*, at 00:44 (YouTube, Feb. 18, 2016), https://www.youtube.com/watch?v=BZmeZyDGkQ0 (on file with the Stanford Law Review).

[8] *Id.* at 02:16; Steve Morgan, *Apple's CEO On Encryption: "You Can't Have A Back Door That's Only for the Good Guys*," FORBES (Nov. 21, 2015, at 06:57 EST), https://www.forbes.com/sites/stevemorgan/2015/11/21/apples-ceo-on-encryption-you-cant-have-a-back-door-thats-only-for-the-good-guys [https://perma.cc/9832-8GWF]; *cf.* Bernstein v. U.S. Dep't of Just., 176 F.3d 1132, 1146 (9th Cir.), *reh'g granted, opinion withdrawn*, 192 F.3d 1308 (9th Cir. 1999) ("Whether we are surveilled by our government, by criminals, or by our neighbors, it is fair to say that never has our ability to shield our affairs from prying eyes been at such a low ebb. The availability and use of secure encryption may offer an opportunity to reclaim some portion of the privacy we have lost.").

[9] MSNBC, Tim Cook's Interview with Chris Hayes and Kara Swisher (Apr. 6, 2018), https://www.ms.now/msnbc/read-tim-cooks-interview-chris-hayes-and-kara-swisher-msna1087436 [https://perma.cc/E9VG-6UH7].

[10] CHARLIE ROSE, *Bill Gates on Apple's iPhone Encryption*, at 01:13 (YouTube, Feb. 22, 2016), https://www.youtube.com/watch?v=nMT0M2PRshY (on file with the Stanford Law Review).

[11] *Id.* at 02:21.

[12] *See, e.g.*, S. 4051, 116th Cong. (2020) (mandating that device manufacturers and service providers "shall ensure that the provider has the ability to provide the assistance . . . decrypting or decoding information . . . or otherwise providing such information in an intelligible format"); David Uberti, *Cybersecurity Experts Take Aim at Senators Over*

statements imploring technology companies to build a so-called backdoor, providing law enforcement with access to encrypted text messages.[13]

The debate intensified in October 2024 following what Senate Intelligence Committee Chair Mark Warner called the "worst telecom hack in our nation's history."[14] Hackers infiltrated Verizon and AT&T systems, enabling them to read Americans' text messages and listen in on live calls.[15] In an unprecedented shift, the FBI—historically opposed to end-to-end encryption—began advising Americans to "stop texting" and use encrypted messaging apps whenever possible.[16] The National Security Agency[17] and the U.S. Cybersecurity and

---

Encryption, WALL ST. J. (July 8, 2020, at 05:30 ET), https://www.wsj.com/articles/cybersecurity-experts-take-aim-at-senators-over-encryption-11594200601 [https://perma.cc/R64U-5W3V]. ("Mandating companies aid law enforcement by decoding encrypted information would effectively require them to build backdoors into their own products . . . .").

[13] *See* Press Release, U.S. Department of Justice, *End-to-End Encryption and Public Safety* (Oct. 11, 2020), https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety [https://perma.cc/UVM5-7GLS]. ("We call on technology companies to work with governments to . . . facilitate legal access in a way that is substantive and genuinely influences design decisions."); Press Release, U.S. Department of Justice, *Attorney General Barr Signs Letter to Facebook from US, UK, and Australian Leaders Regarding Use of End-to-End Encryption* (Oct. 3, 2019), https://www.justice.gov/archives/opa/pr/attorney-general-barr-signs-letter-facebook-us-uk-and-australian-leaders-regarding-use-end [https://perma.cc/D8TD-HHGB]. ("Use of end-to-end encryption, which allows messages to be decrypted only by end users, leaves service providers unable to produce readable content in response to wiretap orders and search warrants . . . . Law enforcement believes it is crucial for technology companies to include lawful access mechanisms in the design of their products or services."). Security researchers characterize such mechanisms as "backdoors." *See* Harold Abelson et al., *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, 1 J. CYBERSECURITY 69, 70 (2015) (describing "law enforcement backdoor" as "a vulnerability open to attack and abuse").

[14] Ellen Nakashima, *Top Senator Calls Salt Typhoon 'Worst Telecom Hack in Our Nation's History'*, WASH. POST (Nov. 21, 2024), https://www.washingtonpost.com/national-security/2024/11/21/salt-typhoon-china-hack-telecom [https://perma.cc/TUE8-JT4V].

[15] *See id.*; Surbhi Misra & David Shepardson, *AT&T, Verizon Targeted by Salt Typhoon Cyberespionage Operation, but Networks Secure*, REUTERS (Dec. 29, 2024, at 00:37 EST), https://www.reuters.com/technology/cybersecurity/chinese-salt-typhoon-cyberespionage-targets-att-networks-secure-carrier-says-2024-12-29/ [https://perma.cc/47KB-H4BE].

[16] Bill Chappell, *FBI Warns Americans to Keep Their Text Messages Secure*, NPR (Dec. 17, 2024, at 05:00 ET), https://www.npr.org/2024/12/17/nx-s1-5223490/text-messaging-security-fbi-chinese-hackers-security-encryption [https://perma.cc/5GZG-58AX].

[17] *See, e.g.*, Mike McConnell, Michael Chertoff & William Lynn, *Why the Fear over Ubiquitous Data Encryption Is Overblown*, WASH. POST (July 28, 2015), https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html [https://perma.cc/3BQH-BTFK] (a former Director of the National Security Agency, a former Secretary of the U.S. Department of Homeland Security, and a former United States Deputy Secretary of Defense jointly writing, "We believe that the greater public good is a secure

Infrastructure Security Agency echoed this guidance, noting that "[e]ncryption is your friend" for texts and phone calls.[18]

At the heart of this debate lies a threshold constitutional question: does encrypted communication fall within the First Amendment's purview?[19] If it does, government restrictions must survive constitutional scrutiny, not the minimal rational basis review that applies to ordinary economic regulations.[20] Without scrutiny, encryption becomes dispensable whenever officials invoke security concerns. With scrutiny, courts must determine whether restrictions are necessary and whether they reach further than required.

The Supreme Court has made historical analysis the cornerstone of First Amendment coverage, treating prior generations' understanding as the decisive factor.[21] The Court asks whether Americans at ratification would have considered a given medium of expression to fall within the Amendment's reach, examining both what governments regulated and what they left alone.[22] Doctrinally speaking, the absence of regulation can be as telling as its presence—when prior generations encountered certain expression without restricting it, that silence suggests they understood it as within the Amendment's purview.[23]

Brown v. Entertainment Merchants Ass'n demonstrates how this works in practice.[24] In that case, California attempted to restrict children's access to violent video games, arguing that interactive digital entertainment—a medium

---

communications infrastructure protected by ubiquitous encryption at the device, server and enterprise level without building in means for government monitoring").

[18] Chappell, *supra* note 16.

[19] This Article deliberately refrains from making normative or prudential claims regarding encryption policy. Instead, it focuses narrowly on analyzing the doctrinal test for First Amendment coverage through the lens of historical analogue methodology.

[20] *See* R.A.V. v. City of St. Paul, 505 U.S. 377, 406 (1992) (White, J., concurring) ("Although the First Amendment does not apply to categories of unprotected speech, such as fighting words, the Equal Protection Clause requires that the regulation of unprotected speech be rationally related to a legitimate government interest.").

[21] *See* Margot E. Kaminski, *Privacy and the Right to Record*, 97 B.U. L. REV. 167, 175–76 (2017) ("In the language of First Amendment scholarship, we often treat First Amendment protection as involving two steps. First, we analyze whether a particular act is 'covered' by the First Amendment . . . . Second, we ask what kind of scrutiny applies to determine whether the expressive act is protected and the regulation fails."); Frederick Schauer, *The Politics and Incentives of First Amendment Coverage*, 56 WM. & MARY L. REV. 1613, 1617–20 (2015) (distinguishing between First Amendment coverage and First Amendment protection).

[22] *See infra* notes 64–67 and accompanying text.

[23] *See* Brown v. Ent. Merchants Ass'n, 564 U.S. 786, 795 (2011).

[24] *See id.*

unimaginable to the Framers—fell outside the First Amendment.[25] The Court disagreed. Video games may be new, but violent entertainment for children was not—Grimms' *Fairy Tales* and Homer's *Odyssey* had circulated freely for centuries—and the absence of regulation established coverage.[26] The same logic applies to encryption: if the Founding generation regularly encrypted their correspondence without government restriction or interference, modern encryption should fall within the First Amendment's scope.

State attorneys general remain divided. Nevada has sued Meta over Facebook Messenger's integration of end-to-end encryption,[27] while California,[28] New York,[29] and the District of Columbia[30] actively encourage residents to use encrypted messaging for sensitive communications. Neither side can cite controlling precedent—the Supreme Court has never addressed encrypted speech under the First Amendment. Courts, in other words, are free to "paint on a blank canvas."[31]

A number of governments around the world have banned, or otherwise restricted, end-to-end encryption.[32] Iran did so in the wake of protests

---

[25] *See id.* at 798 ("California claims that video games present special problems because they are 'interactive.'").

[26] This Article's discussion of violent video games and *Brown* merely reflects an analysis of existing First Amendment doctrine and should not be interpreted as endorsing or condoning violence in video games or other media.

[27] *See* Complaint at 49–51, State of Nevada v. Meta Platforms, Inc., No. A-24-886110-B (Nev. Dist. Ct. Clark Cnty. Jan. 30, 2024).

[28] *See* Press Release, State of Calif. Dep't of Just., Off. of the Att'y Gen., *Consumer Alert with Tips for Protecting Your Privacy* (Sep. 16, 2022), https://oag.ca.gov/news/press-releases/california-attorney-general-bonta-issues-consumer-alert-tips-protecting-your [https://perma.cc/NRK3-XKND]. ("For messaging, only use 3rd party apps that use end-to-end encryption, instead of your phone's default messaging service.").

[29] *See* Press Release, Off. of the N. Y. State Att'y Gen., *AG James Offers Tips to Limit Unwanted Sharing of Personal Information* (May 13, 2022), https://ag.ny.gov/press-release/2022/consumer-alert-attorney-general-james-provides-guidance-protect-digital-privacy [https://perma.cc/C4QP-GYDT] ("Send Messages via End-to-End Encrypted Platforms . . . . End-to-end encryption is designed to ensure that only you and the recipient of your message can see the contents of your message, so it makes it difficult for any third party to spy on your messages.").

[30] *See* Press Release, Off. of the Att'y Gen. for D.C., *Avoid Using Unencrypted Messaging Sites* (Oct. 19, 2022), https://oag.dc.gov/release/consumer-alert-avoid-using-unencrypted-messaging [https://perma.cc/3BQH-BTFK] ("If you do need to discuss sensitive information in texts or online messages, use a secure, encrypted messaging app.").

[31] Gunn v. Minton, 568 U.S. 251, 258 (2013).

[32] *Cf.* Hum. Rts. Council, Rep. of the Off. of the U.N. High Comm'r for Hum. Rts. on its Fifty-First Session, at 6, U.N. Doc. A/HRC/51/17 (Aug. 4, 2022), https://documents.un.org/doc/undoc/gen/g22/442/29/pdf/g2244229.pdf ("In recent years, various Governments have taken actions . . . undermining the security and confidentiality of

following the death of Mahsa Amini, a twenty-two-year-old Kurdish woman who was reportedly beaten to death by Iran's morality police for allegedly violating strict hijab rules.[33] Russia has similarly prevented messaging applications from offering end-to-end encryption to their Russian users, although the European Court of Human Rights has rejected the Russian law, holding that "it impairs the very essence of the right to respect for private life under Article 8 of the [European] Convention [on Human Rights]."[34]

Although the United States is not a signatory to the European Convention on Human Rights, it is bound by constitutional guarantees articulated in the First Amendment. The Supreme Court has declared that the First Amendment covers, in essence, all speech apart from "well-defined and narrowly limited" forms that the nation has a history of regulating.[35] Examples of historically

---

encrypted communications. This has concerning implications for the enjoyment of the right to privacy and other human rights. Encryption is a key enabler of privacy and security online and is essential for safeguarding rights, including the rights to freedom of opinion and expression, freedom of association and peaceful assembly, security, health and non-discrimination.").

[33] *See* Hana Kiros, *Big Tech Could Help Iranian Protesters by Using an Old Tool*, MIT TECH. REV. (Nov. 11, 2022), https://www.technologyreview.com/2022/11/11/1063107/big-tech-iran-protests-domain-fronting [https://perma.cc/6CFD-W3SV].

[34] Podchasov v. Russia, App. No. 33696/19, ¶ 80 (Feb. 13, 2024); https://hudoc.echr.coe.int/eng?i=001-230854 [https://perma.cc/BF4T-88Z2]. ("Weakening encryption by creating backdoors would apparently make it technically possible to perform routine, general and indiscriminate surveillance of personal electronic communications. Backdoors may also be exploited by criminal networks and would seriously compromise the security of all users' electronic communications. The Court takes note of the dangers of restricting encryption described by many experts in the field."). The Russian Federation withdrew from the European Convention on Human Rights in September 2022, but the European Court of Human Rights retains jurisdiction over cases alleging violations before that date. *See* Eur. Ct. H.R., *Resolution of the European Court of Human Rights on the Consequences of the Cessation of Membership of the Russian Federation to the Council of Europe in Light of Article 58 of the European Convention on Human Rights* ¶ 2 (Mar. 22, 2022), https://www.echr.coe.int/documents/d/echr/Resolution_ECHR_cessation_membership_Russia_CoE_ENG [https://perma.cc/5BG9-E3AJ].

[35] United States v. Stevens, 559 U.S. 460, 468–69 (2010) (citations omitted) ("From 1791 to the present . . . the First Amendment has permitted restrictions upon the content of speech in a few limited areas, and has never included a freedom to disregard these traditional limitations."); *cf.* Nat'l Republican Senatorial Comm. v. FEC, 117 F.4th 389, 399 (6th Cir. 2024) (Thapar, J., concurring) ("[A] litigant challenging a law on First Amendment grounds must show that his proscribed conduct has some speech or press element. And he must show that his speech doesn't fall into one of the 'historic and traditional categories' of expression—like obscenity or defamation—that are outside 'the freedom of speech' as the founding generation understood it."), *cert. granted*, 145 S. Ct. 2843 (June 30, 2025).

regulated speech include obscenity,[36] defamation,[37] incitement,[38] fraud,[39] and true threats of violence.[40]

The Court has left the door open to additional unprotected categories—including perhaps encrypted speech—but has placed the burden on the government to demonstrate a history of regulation.[41] That burden is meaningfully eased if the government can establish that encrypted speech is enabled only by recent technological advances and could not have been regulated historically.[42] Indeed, some scholars presume that impenetrable encryption is a late twentieth-century innovation that could not have been anticipated by prior generations of Americans.[43]

This Article challenges that presumption by offering a careful and comprehensive review of Founding-era records preserved in the National Archives, the Library of Congress, and the private libraries of the First Amendment's drafters.[44] Those who ratified the First Amendment, it turns out, were quite familiar with encrypted communication, spurred by the insecurity

---

[36] Roth v. United States, 354 U.S. 476, 484 (1957) ("[I]mplicit in the history of the First Amendment is the rejection of obscenity.").

[37] Beauharnais v. Illinois, 343 U.S. 250, 254–55 (1952) (noting that "[l]ibel of an individual was . . . criminal in the colonies").

[38] Brandenburg v. Ohio, 395 U.S. 444, 447–49 (1969).

[39] Va. Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 771 (1976) (explaining that fraud "has never been protected" under the First Amendment).

[40] *See* Counterman v. Colorado, 600 U.S. 66, 74 (2023); see also United States v. Alvarez, 567 U.S. 709, 718 (2012) ("These categories have a historical foundation in the Court's free speech tradition. The vast realm of free speech and thought always protected in our tradition can still thrive, and even be furthered, by adherence to those categories and rules.").

[41] *See Alvarez*, 567 U.S. at 722 (quoting United States v. Stevens, 559 U.S. 460, 473 (2010)) ("[P]erhaps there exist 'some categories of speech that have been historically unprotected . . . but have not yet been specifically identified or discussed . . . in our case law.'"); Brown v. Ent. Merchants Ass'n, 564 U.S. 786, 792 (2011) (explaining that "without persuasive evidence that a novel . . . is part of a long (if heretofore unrecognized) tradition," a legislature may not regulate it).

[42] *See Brown*, 564 U.S. at 792 (considering California's argument that interactive digital entertainment—a medium unimaginable to the Framers—fell outside the First Amendment). The Court's analysis suggests that if a medium genuinely were new, such that no historical analogue existed and no tradition of non-regulation could be established, a State might more plausibly argue that the lack of historical regulation reflects technological impossibility rather than constitutional commitment.

[43] *See* John A. Fraser III, *The Use of Encrypted, Coded and Secret Communications Is an "Ancient Liberty" Protected by the United States Constitution*, 2 VA. J.L. & TECH. 2, 81 n.4 (1997).

[44] *Cf.* Jud Campbell, *Natural Rights and the First Amendment*, 127 YALE L.J. 246, 263 (2017) ("Recovering the history of expressive freedom . . . has potentially dramatic consequences for legal doctrine.").

of the fledgling postal system. Given the risks inherent to written communication at the time, Americans at the Founding were perhaps more skilled users of encryption than any subsequent generation. Archival records demonstrate that American doctors, lawyers, businessmen, and political leaders turned to encrypted writing in the form of ciphers and codes as an essential, albeit time-consuming and sometimes frustrating, aspect of political life.

Part II of this Article elaborates on the Supreme Court's historical approach to First Amendment coverage and demonstrates its application to encrypted communication. After examining the Court's guidance for reasoning by historical analogue, this Part documents the methodological procedures inherent to Founding-era ciphers and codes. It finds that a number of Founding-era encryption techniques, including one invented by Thomas Jefferson, remained impenetrable well into the twentieth century, even by the most sophisticated government actors.[45]

Part III of this Article explores Founding-era concerns regarding post office security and chronicles the widespread publication of eighteenth-century encryption treatises, including one by the nation's first Postmaster General, Benjamin Franklin.[46] It continues with a review of the rationales offered by America's leading Founders for their insistence on encrypted letters. Ironically, though understandably when viewed in context, archival records show that Bill of Rights author James Madison debated the text of the First Amendment via encrypted messages sent across the Atlantic to Jefferson during his time as U.S.

---

[45] *See* Letter from Thomas Jefferson to Robert Patterson (Mar. 22, 1802), *in* 37 THE PAPERS OF THOMAS JEFFERSON 107–09 (Barbara B. Oberg ed., 2010); RALPH WEBER, MASKED DISPATCHES: CRYPTOGRAMS AND CRYPTOLOGY IN AMERICAN HISTORY, 1775–1900, at 65 (2012) (observing that Jefferson devised an encryption device that was impenetrable to any cryptographic attack of its time).

[46] *See* GEORGE FISHER, THE AMERICAN INSTRUCTOR: OR YOUNG MAN'S BEST COMPANION 54–56 (Phila., New-Printing-Office 1748) (discussing techniques for secret correspondence); *see also* Advice to a Young Tradesman (July 21, 1748), *in* 3 THE PAPERS OF BENJAMIN FRANKLIN 304–08 (Leonard W. Labaree ed., 1961) ("George Fisher's *The Instructor: or Young Man's Best Companion* was a popular manual of English grammar, penmanship, composition, arithmetic, bookkeeping, and other useful matters for young men entering business . . . . [I]t was first published in London in 1730 or earlier . . . . Franklin imported two dozen copies in 1745; in 1747 he began to get an American edition ready."); Letter from Benjamin Franklin to Samuel Franklin (July 7, 1773), *in* 20 THE PAPERS OF BENJAMIN FRANKLIN 277 n.2 (William B. Willcox ed., 1976) ("The 'little Piece of mine' was probably 'Advice to a Young Tradesman' . . . included in George Fisher, *The American Instructor: or Young Man's Best Companion* (Philadelphia, 1748); Samuel's reply below, Dec. 17, acknowledged a 'book of advice.'").

minister to France.[47] An insistence on encrypted communication also permeated the early judiciary, as demonstrated by preserved records from the private library of John Jay, the nation's first Chief Justice.[48] This Part goes on to examine the role of encryption in the formation of Democratic-Republican societies and the emergence of the nation's first opposition party led by Jefferson and Madison.

In short, the historical record shows that the Founders did not treat encryption as an eccentric luxury or mathematical curiosity. They treated it as an instrument of civic and personal life—an ordinary, sometimes tedious practice by which citizens carved out space for candor in their communications. They encrypted despite the frustrations, despite the errors, despite the hours spent decoding garbled messages. They persisted because they understood what was at stake: the capacity to think aloud on paper without an audience of postmasters, magistrates, or political rivals reading over one's shoulder.

Today the medium has changed—the parchment and ink have yielded to keypads and touchscreens, the wooden cipher wheels to silicon processors—but the constitutional stakes remain unchanged. If courts recognize this continuity, they should treat regulations on encryption not as technical policy questions best left to legislative judgment, but as intrusions onto terrain the First Amendment was designed to protect. That recognition does not leave encryption immune to regulation. It would simply insist that any move to read what citizens write in confidence to one another must face the scrutiny that the First Amendment demands. The government, in other words, must justify, not merely announce, its authority to intercept Americans' private communications.

---

[47] *See, e.g.*, Letter from Thomas Jefferson to James Madison (Jan. 31, 1783), *in* 6 THE PAPERS OF JAMES MADISON 177–82 (William T. Hutchinson & William M. E. Rachal eds., 1969) ("The present letter makes clear that Jefferson, before leaving Philadelphia . . . had 'concerted' with [James Madison] in preparing a code for the greater security of confidential portions of their correspondence."); Letter from James Madison to Thomas Jefferson (May 27, 1789), *in* 12 THE PAPERS OF JAMES MADISON 185–87 (Charles F. Hobson & Robert A. Rutland eds., 1979) ("Italicized words are those encoded by [James Madison] using the code Jefferson sent him on 11 May 1785. Decoded interlinearly by Jefferson."); Letter from Thomas Jefferson to James Madison (Aug. 28, 1789), *in* 15 THE PAPERS OF THOMAS JEFFERSON 364–69 n.2 (Julian P. Boyd ed., 1958) ("This and subsequent words in italics . . . are written in code and were decoded interlineally by Madison; his decoding has been verified by the Editors, employing Code No. 9.").

[48] *See, e.g.*, Letter from John Jay to William Carmichael (Jan. 27, 1780), *in* 2 THE SELECTED PAPERS OF JOHN JAY 18–21 (Elizabeth M. Nuxoll ed., 2012) ("You will oblige me by being very regular & circumstantial in your Correspondence, and commit Nothing of a private Nature to Paper unless in Cypher.").

II. ENCRYPTION AS THE REEMERGENCE OF WIDESPREAD EIGHTEENTH-CENTURY PRACTICES

Emerging technologies often raise novel questions about the First Amendment's reach.[49] Whether the Amendment encompasses encrypted communications determines everything that follows: the tests courts apply, the burden the government bears, and the degree of protection encryption receives.[50]

If encrypted communication lies outside the Amendment's reach, restrictions will be judged under the deferential standard applied to ordinary economic regulation—an inquiry that asks only whether the restriction is rationally related to some legitimate government purpose.[51] That low bar is easily cleared so long as the government proclaims an interest in accessing encrypted communications.

If encrypted speech falls within the First Amendment's purview, however, the government cannot simply announce law enforcement needs and expect deference. Courts must ask whether regulation is necessary, whether alternative measures could achieve the same ends, and whether the scope of intrusion exceeds what the government's interests can justify.[52]

The precise level of scrutiny—strict or intermediate—will depend on how a particular restriction is framed, whether it targets content or merely conduct.[53] But the essential point remains: rational-basis review cannot suffice for restrictions that pierce the confidentiality of encrypted communications.

---

[49] *See*, *e.g.*, United States v. Paramount Pictures, Inc., 334 U.S. 131, 166 (1948) ("We have no doubt that moving pictures, like newspapers and radio, are included in the press whose freedom is guaranteed by the First Amendment."); cf. Michael W. McConnell, Reconsidering Citizens United as a Press Clause Case, 123 Yale L.J. 412, 428 (2013) ("As the technology for dissemination of ideas and opinions to the public has advanced, from the printing press to radio to television to film to the internet, blogs, Twitter, and video games, the Supreme Court has quite properly . . . extended the principle of freedom of the press to the various media for the dissemination of opinion and information to the general public.").

[50] *See* Schauer, *supra* note 21, at 1617 ("In order to understand the question of coverage and to appreciate its importance, it is necessary to distinguish the idea of coverage from that of protection."); Kaminski, *supra* note 21, at 175–76.

[51] *See* R.A.V. v. City of St. Paul, 505 U.S. 377, 383 (1992) ("We have sometimes said that these categories of expression are not within the area of constitutionally protected speech or that the protection of the First Amendment does not extend to them.").

[52] *See*, *e.g.*, Brown v. Ent. Merchants Ass'n, 564 U.S. 786, 799 (2011) (applying strict scrutiny to California statute after establishing First Amendment coverage for video games); United States v. Stevens, 559 U.S. 460, 472 (2010) (applying strict scrutiny to federal statute after establishing First Amendment coverage for depictions of animal cruelty).

[53] *Cf.* Kaminski, *supra* note 21, at 173 ("When First Amendment coverage extends to a

Courts typically define the scope of constitutional rights through linguistic analysis. While terms like "seizure" in the Fourth Amendment and "punishment" in the Eighth Amendment help delineate those rights' boundaries, the First Amendment's reference to "speech" provides limited guidance. Legal scholars have long recognized the futility of relying on dictionary definitions of "speech" to determine First Amendment scope.[54] As Justice Holmes observed more than a century ago, "the First Amendment . . . cannot have been, and obviously was not, intended to give immunity for every possible use of language."[55] Fraudulent speech, for example, surely falls outside the Amendment's scope, despite its reliance on verbal or written expression.[56]

Instead, the Supreme Court has anchored First Amendment coverage in historical practice. To place expression outside the Amendment's reach, the government must prove prior generations placed it there first. As the Court has reiterated a number of times over the past two decades, both in holdings and dicta, "the government must generally point to *historical* evidence about the reach of the First Amendment's protections" to deny coverage.[57]

---

particular activity, the fear is that courts will apply strict scrutiny, which is famously 'fatal in fact,' or some other form of heightened speech scrutiny under which the regulations are doomed to fail.").

[54] *See, e.g.*, Schauer, *supra* note 21, at 1619 ("If the coverage of the First Amendment were even close to the ordinary meaning of the word "speech," then vast segments of human life would remain shielded by the First Amendment from regulation or other legal consequences."); Frederick Schauer, *The Boundaries of the First Amendment: A Preliminary Exploration of Constitutional Salience*, 117 HARV. L. REV. 1765, 1773 (2004) ("That the boundaries of the First Amendment are delineated by the ordinary language meaning of the word 'speech' is simply implausible.").

[55] Frohwerk v. United States, 249 U.S. 204, 206 (1919).

[56] *See* Schauer, *supra* note 54, at 1778 ("A prime example of speech residing almost imperceptibly outside the First Amendment's boundaries is the speech that is the primary target of federal securities regulation.").

[57] *E.g.*, N.Y. State Rifle & Pistol Ass'n, Inc. v. Bruen, 597 U.S. 1, 24–25 (2022); *see also* City of Austin v. Reagan Nat'l Advert. of Austin, LLC, 596 U.S. 61, 75–76 (2022) (recognizing "history and tradition of regulation" as relevant when considering the scope of the First Amendment); Williams-Yulee v. Fla. Bar, 575 U.S. 433, 446 (2015) ("[A] history and tradition of regulation are important factors in determining whether to recognize 'new categories of unprotected speech.'"); Brown v. Ent. Merchants Ass'n, 564 U.S. 786, 792 (2011); United States v. Stevens, 559 U.S. 460, 468–70 (2010). Even dissenting Justices acknowledge that, in the context of First Amendment coverage, history is the north star. *See, e.g.*, *Bruen*, 597 U.S. at 106 (Breyer, J., dissenting) ("[W]e do look to history in the First Amendment context to determine whether the expressive conduct falls outside of the category of protected speech."); *Williams-Yulee*, 575 U.S. at 462 (Scalia, J., dissenting) ("Our cases hold that speech enjoys the full protection of the First Amendment unless a widespread and longstanding tradition ratifies its regulation.").

The Court presumes that if prior generations regulated certain speech without constitutional objection, then Americans must have understood that form of speech to fall outside the First Amendment's scope.[58] The burden of proof, however, rests with the government. It must demonstrate clear evidence of historical regulation.[59] If the government cannot muster records showing a longstanding tradition of restricting the type of content at issue, courts will subject new speech restrictions to First Amendment scrutiny.

The Court's decision in *Brown v. Entertainment Merchants Ass'n* illustrates this approach.[60] *Brown* involved a First Amendment challenge to California's restrictions on children's access to violent video games. California argued that video games—as interactive entertainment unknown to the First Amendment's framers—fell outside constitutional protection and could be distinguished from protected media like books, plays, and films.[61]

The state's argument failed, however, because it could not identify historical precedent for denying First Amendment coverage to violent entertainment. While the challengers acknowledged video games' novelty, they successfully demonstrated that concerns about violence in children's entertainment dated back centuries.[62] The Court, in a 7-2 decision, found video games within the First Amendment's scope and subject to strict scrutiny, analogizing them to choose-your-own-adventure books that had been in circulation for generations.[63]

---

[58] Some scholarship suggests the founding generation might have conceptualized First Amendment freedom of speech through the lens of natural rights, which could be regulated for the public good. *See, e.g.*, Campbell, *supra* note 44, at 252. This Article examines what might be termed the historical analogue approach, which emphasizes concrete evidence of past speech regulation rather than natural rights theory, while acknowledging the complexity and uncertainty surrounding its development and application.

[59] *See, e.g.*, United States v. Playboy Ent. Grp., Inc., 529 U.S. 803, 816 (2000) ("When the Government restricts speech, the Government bears the burden of proving the constitutionality of its actions."); *Bruen*, 597 U.S. at 24–25 ("[T]o carry that burden, the government must generally point to historical evidence about the reach of the First Amendment's protections.").

[60] *See Brown*, 564 U.S. at 792.

[61] *See id.* at 798 ("California claims that video games present special problems because they are 'interactive,' in that the player participates in the violent action on screen and determines its outcome.").

[62] *See id.* at 795–96 ("Certainly the books we give children to read—or read to them when they are younger—contain no shortage of gore.").

[63] *See* Brown v. Ent. Merchants Ass'n, 564 U.S. 786, 798 (2011) ("[Y]oung readers of choose-your-own-adventure stories have been able to make decisions that determine the plot by following instructions about which page to turn to.").

The Court emphasized the absence of historical precedent for California's position: "California's argument would fare better if there were a longstanding tradition in this country of specially restricting children's access to depictions of violence, but there is none."[64] To illustrate this point, the Court catalogued violent content in children's literature across centuries, from Grimms' *Fairy Tales*—where a wicked queen dances to death in burning slippers and Cinderella's stepsisters have their eyes pecked out by doves—to standard high school texts like Homer's *Odyssey* and Dante's *Inferno*.[65]

Some critique the Court's approach in *Brown*, arguing that the absence of regulation shouldn't automatically establish constitutional protection. They note the Court's analysis lacks traditional evidence of original intent—no citations to ratifying conventions or Founding-era treatises linking free speech to violent children's literature.[66] The *Brown* majority, however, set a lower evidentiary bar: First Amendment coverage requires only that prior generations encountered analogous expression without restricting it or treating it as constitutionally unprotected.[67]

How does this framework apply to encrypted text messaging? Courts would look for evidence that prior generations encountered analogous expression that was either left unregulated or regulated consistent with First Amendment principles. The historical analogue is already settled: the Court has held that an electronic message corresponds to a "note" or "letter" for First Amendment purposes.[68] The critical question thus narrows: Did prior generations of Americans encounter encrypted notes or letters? And if so, did they treat them as falling outside the First Amendment's scope?

The absence of regulation carries particular weight. Just as *Brown* found meaning in the lack of historical restrictions on violent children's literature, the absence of colonial or early American limitations on encrypted letters would support First Amendment coverage. Widespread use by prominent figures, particularly without government interference, would reinforce that conclusion. Conversely, if the historical record reveals that encrypted communications

---

[64] *See id.* at 795.

[65] *See id.* at 796.

[66] *See id.* at 821–22 (Thomas, J., dissenting) ("The Court's decision today does not comport with the original public understanding of the First Amendment.").

[67] *See id.* at 795–98.

[68] Reno v. ACLU, 521 U.S. 844, 851 (1997) ("E-mail enables an individual to send an electronic message—generally akin to a note or letter—to another individual or to a group of addressees.").

were rare, viewed with suspicion, or primarily associated with criminal activity, courts may be less inclined to recognize such practices as a meaningful historical analogue.

The government might argue that modern encryption differs fundamentally from its historical antecedents in accessibility—that eighteenth-century ciphers required training and effort, while today's encryption operates invisibly at the touch of a button. *Brown* forecloses this argument. Technological advancement alone cannot strip constitutional protection from expression that enjoys historical recognition.[69] Just as the Court rejected attempts to distinguish video games from violent literature, it would likely resist efforts to separate modern encryption from Founding-era ciphers based purely on convenience.

One of the drawbacks of history as an interpretive methodology is its so-called "workability." As Justice Jackson has noted, "sift[ing] through troves of centuries-old documentation looking for supportive historical evidence" is "no small thing to [lower] courts with heavier caseloads and fewer resources than we have."[70]

This Article seeks to ease the burden on jurists as they are called to consider a First Amendment question particularly salient to the more than 300 million smartphone users in the United States.[71] Although encryption is often thought of as the domain of the mathematically or technologically inclined, advancements in computing technology have brought to it an astonishing degree of convenience.[72] In enabling end-to-end encryption by default, mobile messaging applications have embedded the methodology into many Americans' daily lives as a virtually invisible security layer safeguarding their

---

[69] *See* Brown v. Ent. Merchants Ass'n, 564 U.S. 786, 790 (2011) ("[W]hatever the challenges of applying the Constitution to ever-advancing technology, the basic principles of freedom of speech and the press, like the First Amendment's command, do not vary when a new and different medium for communication appears.").

[70] United States v. Rahimi, 602 U.S. 680, 741 (2024) (Jackson, J., concurring) ("I write separately because . . . the experiences of courts applying its history-and-tradition test should bear on our assessment of the workability of that legal standard.").

[71] Carpenter v. United States, 585 U.S. 296, 300 (2018) ("There are 396 million cell phone service accounts in the United States—for a Nation of 326 million people.").

[72] *See* Eli Lake, *Government Is Fighting Itself on Encryption*, BLOOMBERG (Sep. 18, 2015, 6:00 AM), https://www.bloomberg.com/view/articles/2015-09-18/government-is-fighting-itself-on-encryption [https://perma.cc/9D3S-DWTX]. (quoting chief technologist Chris Soghoian: "What's amazing about this next generation of secure communication tools, is not just that they employ best-of-breed cryptography . . . . It's that they are now easy to use.").

private communications.[73] The convenience may be new, but the practice itself is not. As this Part demonstrates, eighteenth-century Americans deployed encryption that was just as impenetrable to government surveillance, even if it required more effort to use.

A. Eighteenth-Century Americans Embraced Encrypted Codes and Ciphers to Safeguard Sensitive Communications

At a basic level, encryption can be understood as scrambling the letters in messages to preserve the confidentiality of a communication.[74] It allows authors to transform plain text into obscure letters, numbers, and symbols.[75] An effective encryption algorithm would allow the intended recipients—and, importantly, no others—to decipher the meaning of seemingly obscure characters.[76] The purpose of going to such lengths is to protect the confidentiality and integrity of the message against third-party access or manipulation. Although encryption can be deployed with a pencil and paper, the assistance of calculators or computers makes the encryption—and, perhaps more importantly, the decryption—process more convenient.[77]

Encryption can be understood in essence as a more advanced form of secret writing.[78] In the eighteenth century, for example, those without the

---

[73] *Id.* ("[M]ajor Internet companies didn't offer powerful encryption as a default setting on their products. That is changing in 2015.").

[74] *See* David B. Walker, *Privacy in the Digital Age: Encryption Policy—A Call for Congressional Action*, 1999 STAN. TECH. L. REV. 3, 14 (1999) ("Encryption is the transformation of data into an unreadable form. Its purpose is to ensure privacy by keeping information hidden from anyone for whom it is not intended, even those who have access to the encrypted data.").

[75] *See* John Jay's Use of Codes and Ciphers, *in* 2 THE SELECTED PAPERS OF JOHN JAY, *supra* note 48, at 7–13 ("[A] definition of basic cryptographic terms: When a passage is not encrypted, it is referred to as 'plaintext.' When a passage is encrypted, generally either a cipher or code is used.").

[76] *See* JENNIFER WILCOX, REVOLUTIONARY SECRETS: CRYPTOLOGY IN THE AMERICAN REVOLUTION 3 (2012) ("Cryptography—the use of ciphers and codes—makes messages unintelligible to an adversary . . . . Theoretically, the adversary . . . could not understand the message even if it were captured.").

[77] Allen Cook Barr, *Guardians of Your Galaxy S7: Encryption Backdoors and the First Amendment*, 101 MINN. L. REV. 301, 306 (2016) ("Fundamentally, there is nothing about computer encryption that could not be accomplished by a human using pencil and paper, given enough time.").

[78] *See* Letter to Thomas Jefferson from Robert Patterson (Dec. 19, 1801), *in* 36 THE PAPERS OF THOMAS JEFFERSON 170–75 (Barbara B. Oberg ed., 2009) ("The art of secret writing, or, as it is usually termed, writing in cypher, has occasionally engaged the attention both of the states-man & philosopher for many ages."); *see also* D. Victoria Baranetsky, *Encryption and the Press Clause*, 6 N.Y.U. J. INTELL. PROP. & ENT. L. 179, 207–08 (2017) ("Based on the Greek words

patience, inclination, or training to encrypt messages used simpler methods to protect the privacy of their letters' contents, such as "wrapping . . . an extra blank sheet around the letter to prevent reading through the paper" or writing in "invisible ink" as George Washington was known to do in his earlier years.[79]

Historically, encryption fell into one of two categories: codes or ciphers.[80] A code substitutes words, phrases, or letters for unreadable numbers or characters according to an agreed upon algorithm. Book codes, for example, were one of the most commonly deployed codes of the Founding era, allowing authors to substitute three numbers for a particular word.[81] Those three numbers corresponded to the word's placement in an agreed-upon book, often a dictionary.[82] The first digit corresponded to the page number, the second digit to the line number, and the third digit to the position of the word in the line.[83]

Abel Boyer's *Royal Dictionary* published in 1771 and John Entick's *New Spelling Dictionary* published in 1777 were popular book code choices in the Founding era.[84] Correspondents often agreed in advance to deliberately shift their numerical references, adding or subtracting a fixed number to obscure the true location of each word, so that even if third parties knew the correct

---

kryptos, meaning hidden or secret, and *graphia*, meaning writing—encryption is inviolably intertwined with all technological communication—dating back to pen and invisible ink.").

[79] Anuj C. Desai, *Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy*, 60 STAN. L. REV. 553, 562 (2007) ("In modern parlance, we might refer to these as technological protection measures—hardly quantum cryptography but certainly technological means for achieving the same end."); WILCOX, *supra* note 76, at 5 ("The use of invisible inks is an ancient art, and the idea of disappearing writing was not new at the time of the American Revolution.").

[80] *Cf.* John Jay's Use of Codes and Ciphers, *supra* note 75, at 7–13 (explaining that the Founders "did not distinguish codes and ciphers, referring to both as 'cyphers'" but that it is nevertheless "useful to understand the differences between these two types of encryption and the proper terminology involved").

[81] *See* MARK T. HOVE, U.S. DEP'T OF STATE, HISTORY OF THE BUREAU OF DIPLOMATIC SECURITY OF THE UNITED STATES DEPARTMENT OF STATE xviii (2011) (noting the commonality of "using the same book to encode a message in which each word was replaced by a number").

[82] *See* John Jay's Use of Codes and Ciphers, *supra* note 75, at 7–13 ("'Book codes' are based on commonly available books, usually dictionaries. A word or letter is substituted by the coordinates of the word or letter within the book: page and line numbers, and indications of columns within a page.").

[83] *See* HOVE, *supra* note 81, at xviii.

[84] *See* John Jay's Use of Codes and Ciphers, *supra* note 75, at 7–13 (observing that John Entick's New Spelling Dictionary "was perhaps the most popular dictionary for cryptography during the [Revolutionary] war"); cf. Letter from William Carmichael to Benjamin Franklin (Feb. 1, 1778), in 25 The Papers of Benjamin Franklin 565–68 (William B. Willcox ed., 1986) (noting that the author took the "precaution of pasting some information . . . in the inside cover of a pocket Dictionary, which he also intended to be made use of as a cypher between" him and Benjamin Franklin).

dictionary, they could not easily decipher the message. For example, Jay is reported to have used a dictionary code that added "23 to the page number and 96 to the line number," in addition to counting "from the bottom right" of the page instead of the more typical top left.[85]

Eighteenth-century Americans considered it best practice to agree upon a code when meeting in person so that instructions on how to unscramble a future correspondence would not be available in writing for prying eyes.[86] Because of the difficulty involved in encrypting text in the eighteenth century, many letters were sent in partially encrypted form with only particularly sensitive sentences or words in a cryptic format. The letter below, sent by Franklin, provides an example of partial encryption typical of the eighteenth century:

> Dear Sir,
>
> We have News here that your Fleet has behaved bravely; I congratulate you upon it most cordially.
> I have just received a 14. 5. 3. 10. 28. 2. 76. 202. 66. 11. 12. 273. 50. 14. joining 76. 5. 42. 45. 16. 15. 424. 235. 19. 20. 69, 580. 11. 150. 27. 56. 35. 104. 652. 28. 675. 85. 79. 50. 63. 44. 22. 219. 17. 60. 29. 147. 136. 41. but this is not likely to afford 202. 55. 580. 10. 227. 613. 176. 373. 309. 4. 108. 40. 19. 97. 309 17. 35. 90. 201. 100. 677.
> By our last Advices our Affairs were in a pretty good train. I hope we shall have advice of the Expulsion of the English from Virginia.
> I am ever, Dear Sir,
> Your most obedient & most humble Servant,
>
> B. Franklin.[87]

---

[85] *See* John Jay's Use of Codes and Ciphers, *supra* note 75, at 7–13 ("Because of the inadequacies of simple ciphers, [John] Jay began proposing book codes in 1780.").

[86] *See*, *e.g.*, *id.* ("Since no extant previous correspondence about this code has been found, [John] Jay and [Gouverneur] Morris probably had agreed upon it before Jay's departure."); Letter from Thomas Jefferson to James Madison (Jan. 31, 1783), in 6 THE PAPERS OF JAMES MADISON, *supra* note 47, at 177–82 ("The present letter makes clear that Jefferson, before leaving Philadelphia for Baltimore, had 'concerted' with [Madison] in preparing a code for the greater security of confidential portions of their correspondence.").

[87] Letter from Benjamin Franklin to Charles Dumas (Aug. 16, 1781), *in* RALPH WEBER, MASKED DISPATCHES: CRYPTOGRAMS AND CRYPTOLOGY IN AMERICAN HISTORY, 1775–1900, 2 (2012); *see id.* at 3 ("The plain text for the enciphered message paragraph was as follows (with original spelling):

Ciphers, by contrast, scramble individual letters according to a mathematical algorithm.[88] A cipher can be as simple as shifting the letters of the alphabet by one digit—writing, for example, "Tvqsfnf Dpvsu" in place of "Supreme Court"—or as complex as computing technology would allow. While simpler ciphers are more convenient to use, they are also comparatively less effective at ensuring the message's content stays private. A sharp mathematical mind, or a computer, can iterate through potential combinations until it finds one that makes the message's content readable.

Encryption technology is continually advancing. In fact, even at the nation's founding—from the Declaration of Independence in 1776 to the Constitutional Convention in 1789—Americans deployed at least seventeen different ciphers, twenty-three different codes, and ten different algorithms which combined features of both ciphers and codes.[89] The state of the art, in other words, does not stand still. It improves as rapidly as mathematical progress allows.

B. Eighteenth-Century Americans Could Deploy Impenetrable Encryption

Whether eighteenth-century encryption is "relevantly similar" to modern encryption depends in large part on what metric the Court applies.[90] If the metric is convenience, for example, the Court may determine that Founding-era encryption is not an appropriate historical analogue.[91] Decrypting a

---

I have just received a neuu commissjon joining me uuith m adams in negociaions for peace but this is not likely to afford me much employ at present.").

[88] The word "ciphers" was more commonly spelled "cyphers" in the eighteenth century. *See generally* WEBER, *supra* note 45, at 2 ("A 'cipher' features the substitution or transposition of individual letters according to a chart or algorithm."); WILCOX, *supra* note 76, at 4 ("Ciphers rearrange letters or change individual letters into a different letter, number, or symbol based on a prearranged setting known as a key."); Kerr, *supra* note 5, at 917 ("A cipher is a method of transforming a text in order to conceal its meaning.").

[89] *See* HOVE, *supra* note 81, at xviii.

[90] N.Y. State Rifle & Pistol Ass'n, Inc. v. Bruen, 597 U.S. 1, 29 (2022) (internal quotation marks and citations omitted) ("[B]ecause everything is similar in infinite ways to everything else, one needs some metric enabling the analogizer to assess which similarities are important and which are not. For instance, a green truck and a green hat are relevantly similar if one's metric is things that are green. They are not relevantly similar if the applicable metric is things you can wear."); *see generally* Cass R. Sunstein, *On Analogical Reasoning Commentary*, 106 HARV. L. REV. 741, 785 (1993) ("[T]he description of relevant similarities and differences will have evaluative dimensions, and these should be made explicit."); *cf.* United States v. Rahimi, 602 U.S. 680, 681 (2024) ("Why and how the regulation burdens the right are central to this inquiry . . . . [A] challenged regulation that does not precisely match its historical precursors still may be analogous enough to pass constitutional muster.").

[91] *Bruen*, 597 U.S. at 30 (explaining that the Court is looking for a "historical analogue, not a

message using pen and paper is much less convenient than a smartphone application that can instantaneously decrypt the same message without any user effort. Archival records suggest that the Founders, in fact, struggled to decrypt messages at times due to their own mistakes in counting, their misunderstanding of the encryption algorithm, or simply their lack of patience with the cumbersome process.[92]

If the relevant metric for comparison, however, is the strength of the encryption algorithms available—as measured by the ability of government authorities to breach the algorithm—then eighteenth-century encryption and its modern counterparts are remarkably similar.[93] Indeed, encryption methodologies were as impenetrable in the Founding era as the most sophisticated algorithms are today.[94] Americans in the late eighteenth century could readily "encrypt letters in ciphers that no government could break."[95] The Vigenère cipher is one such example. It was popularized in the seventeenth century and remained impenetrable for many decades after the Founding.[96]

Before taking office as President in 1801, Jefferson invented an encryption device for personal use that "would almost certainly have withstood any cryptographic attack" by even the most sophisticated government actors of the era.[97] Jefferson referred to his device, depicted in **Figure 1**, as a "wheel cypher" in a letter describing its operation to his friend Dr. Robert Patterson, a mathematics professor at the University of Pennsylvania.[98] Although the exact

---

historical twin"—"even if a modern-day regulation is not a dead ringer for historical precursors, it still may be analogous enough to pass constitutional muster.").

[92] *See infra* notes 157–173.

[93] *See generally* WEBER, *supra* note 45, at 13 ("[T]he art of cryptology had become quite sophisticated by 1775 . . . .").

[94] Although the sophistication of encryption techniques has no doubt increased in the intervening almost two and a half centuries with the advent of computing technology, the newfound computing power can similarly be harnessed by government authorities to breach user encrypted messages.

[95] A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. Pa. L. Rev. 709, 798 (1995).

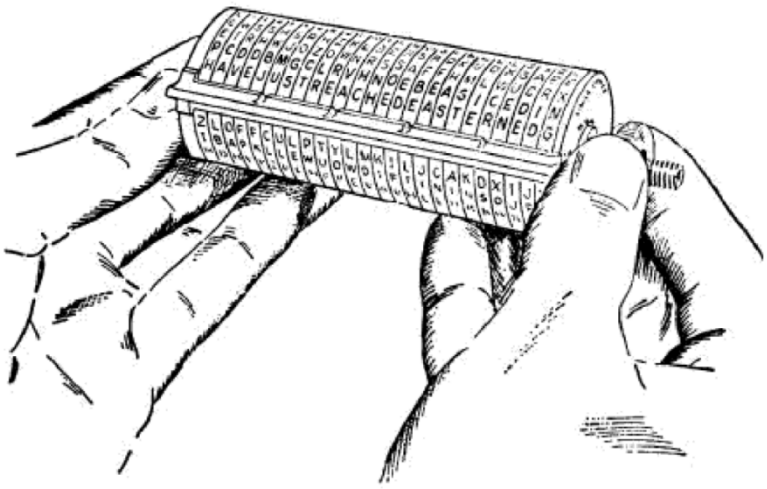
[96] *See id.* at 845 ("Letters could be encoded with the then-unbreakable Vigenère cipher . . . . Strong cryptography offers the prospect of restoring the privacy enjoyed by Jefferson and Adams . . . thereby making it again possible to enjoy this privacy, albeit with a larger number of correspondents spread out over greater distances."); *see also* DAVID KAHN, THE CODEBREAKERS 214–21 (1967) (referring to the Vigenère cipher and its long-standing reputation as "le chiffre indéchiffrable," or the indecipherable cipher).

[97] KAHN, *supra* note 96, at 195; *see also* WEBER, *supra* note 45, at 65 (identifying Jefferson as the "Father of American Cryptography" and his wheel cypher as among the most advanced of the era).

[98] Letter from Thomas Jefferson to Robert Patterson (Mar. 22, 1802), *in* 37 THE PAPERS OF

year of his invention is subject to some debate among historians—either between 1790 and 1793 or between 1797 and 1800—the device was considered impenetrable by even the most sophisticated government agencies well into the twentieth century.[99] In fact, more than a century after its invention, in 1922, "the U.S. Army adopted an almost identical device that ha[d] been independently invented."[100] The Jefferson wheel cypher reportedly remained in use by the U.S. Navy as late as 1967.[101]

Figure 1: "Wheel Cypher" Invented by Thomas Jefferson Prior to His Presidency and Implemented by the U.S. Army in 1922 [102]



THOMAS JEFFERSON, *supra* note 45, at 107–09; *cf.* Description of a Wheel Cipher (before Mar. 22, 1802), *in* 37 THE PAPERS OF THOMAS JEFFERSON, *supra* note 45, at 102–07 ("[A] passing reference to 'my wheel cypher' in TJ's letter to Robert Patterson on 22 Mch. 1802 is apparently the only time he mentioned the cryptographic device in his correspondence."); KAHN, *supra* note 96, at 214 ("Jefferson's explanation of the wheel cypher is characteristically clear and economical . . . ."); *World's Oldest True Cipher Device, the "Jefferson Cipher," on Display at the National Cryptologic Museum*, NAT'L SEC. AGENCY (Dec. 19, 2022), https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3250041/worlds-oldest-true-cipher-device-the-jefferson-cipher-on-display-at-the-nationa/ [https://perma.cc/6TM8-VYNQ] ("Jefferson corresponded frequently with Robert Patterson, a professor of mathematics at the University of Pennsylvania and fellow member of the American Philosophical Society.").

[99] KAHN, *supra* note 96, at 214–16; *see also* WEBER, *supra* note 45, at xii (referring to Jefferson's "wheel cypher" as "twentieth-century security, for secret messages").

[100] KAHN, *supra* note 96, at 195; *see id.* at 214–16 ("Later, other branches of the American government used the Jefferson system, generally slightly modified, and it often defeated the best efforts of the 20th-century cryptanalyst who tried to break it . . . .").

[101] *See* Froomkin, *supra* note 95, at 799 n.372; KAHN, *supra* note 96, at 192–95.

[102] KAHN, *supra* note 96, at 194.

The device's novelty lay not only in its encryption method, but also in its convenience. It featured cylindrical wooden pieces on an iron spindle that allowed for handheld operation, making the encryption and decryption process readily available to those without the patience or training for manual computation.[103] Jefferson's device, in other words, aided in the otherwise laborious process of encrypting and decrypting messages by making it as straightforward as turning wooden wheels with the letters of the alphabet marked on their edges.[104]

In fact, papers discovered by the Library of Congress in 1922 indicate that Jefferson thought deeply about ensuring that the handheld operation was as user-friendly as possible, noting that six inches for the cylinder "probably will be a convenient length as it may be spanned between the middle ring & thumb of the left hand, while in use."[105] Jefferson's focus on convenience—reducing encryption from a laborious manual process to simply turning wooden wheels—reflects a broader trajectory in which each generation of encryption technology has prioritized ease of use, culminating in encryption so seamless that modern users do not even know it's happening.

III. A VULNERABLE POSTAL SYSTEM SPARKED THE FOUNDERS' INTEREST IN ENCRYPTED LETTERS

Accessing the volume and breadth of historical records examined in this Article is feasible thanks to joint efforts by those at the National Archives, the Library of Congress, and a number of presidential libraries across the country. These institutions have preserved and made accessible documents central to the nation's Founding and early development, including previously overlooked correspondence and records that shed light on early American communication security practices.[106] As legal historians have noted, the past two decades have

---

[103] WEBER, *supra* note 45, at 62 ("Jefferson's cipher cylinder promised more prompt and efficient enciphered communications, provided the devices could be safely delivered to the correspondents.").

[104] *See* Description of a Wheel Cipher (before Mar. 22, 1802), *supra* note 98, at 102–07.

[105] *Id.*; *see also* KAHN, *supra* note 96, at 216 (noting that the U.S. Army adopted Jefferson's wheel cypher as the M-94 field cipher in 1922).

[106] *See* Kathleen Williams, *The NHPRC: Extending the Archives' Reach*, 41 NAT'L ARCHIVES & RECS. ADMIN. PROLOGUE (2009), https://www.archives.gov/publications/prologue/2009/summer/nhprc.html [https://perma.cc/2MHP-5S97] (noting that NHPRC-funded archival projects "reveal 'hidden

witnessed transformative changes in archival accessibility, fundamentally altering how scholars can engage with primary sources from the Founding era.[107] This technological revolution in archival access has made possible previously impractical lines of historical inquiry and enabled new approaches to analyzing early American documents.[108]

The growing accessibility of archival sources may help address persistent concerns about the practicality of using historical analysis in constitutional interpretation.[109] Even in instances where the record remains fragmentary, the Justices have recognized that historical evidence can, at minimum, help narrow the range of plausible interpretations of vague constitutional text.[110] The rich historical record on early American encryption practices and privacy norms offers precisely this kind of interpretive guidance.

---

collections' by processing backlogs" and that early attempts to collect Founders' papers "were flawed because they ignored documents hidden in private collections or those outside of federal stewardship").

[107] Alexandra Chassanoff, *Historians and the Use of Primary Source Materials in the Digital Age*, 76 AM. ARCHIVIST 458, 459 (2013); *see also* Wanling Su, *What Is Just Compensation?*, 105 VA. L. REV. 1483, 1488 (2019) ("[T]he digitization of these records is a recent phenomenon, only possible thanks to advancements in imaging technology and the development of academic libraries."); *cf.* Paul Finkelman, *Thomas Jefferson, Original Intent, and the Shaping of American Law: Learning Constitutional Law from the Writings of Jefferson*, 62 N.Y.U. ANN. SURV. AM. L. 45, 48 (2006) ("While familiar to historians, the massive and incredibly valuable collections of the papers of the Founders are often unknown to legal scholars.").

[108] *See* Su, *supra* note 107, at 1522; Lara Putnam, *The Transnational and the Text-Searchable: Digitized Sources and the Shadows They Cast*, 121 AM. HIST. REV. 377, 379 (2016) ("Precisely because web-enabled digital search simply accelerates the kinds of information-gathering that historians were already doing, its integration into our practice has felt smooth rather than revolutionary. But increasing reach and speed by multiple orders of magnitude is transformative. It makes new realms of connection visible, new kinds of questions answerable.").

[109] *See*, *e.g.*, United States v. Rahimi, 602 U.S. 680, 741–42 (2024) (Jackson, J., concurring) ("In my view, as this Court thinks of, and speaks about, history's relevance to the interpretation of constitutional provisions, we should be mindful that our common-law tradition of promoting clarity and consistency in the application of our precedent also has a lengthy pedigree. So when [lower] courts signal they are having trouble with one of our [historical] standards, we should pay attention.").

[110] *Id.* at 734 (Kavanaugh, J., concurring); *see also* Nikolas Bowie, *The Constitutional Right of Self-Government*, 130 Yale L.J. 1652, 1725 (2021) ("Uncovering alternative possibilities is particularly important with respect to texts, whose setting—historical, cultural, authorial—constrains and delimits the viable interpretations that these texts are able to bear. For any text, an appreciation of the context and larger possibilities behind it does help in understanding it.").

A. The Nation's First Postmaster General Championed Confidential Correspondence

Coming across an encrypted letter in the mail would not raise eyebrows among eighteenth-century Americans.[111] Due to the fraught nature of postal transit in early America, political and business leaders in the emerging republic were customarily trained to encrypt sensitive letters.[112] Encryption offered the only reliable guarantee of a letter's security against interception en route or an untrustworthy courier.

In the Founding era, letters were typically sent without an envelope. The sender would simply fold the pages over and then seal them in wax to preserve some semblance of confidentiality. But the wax "seals often fell apart during transit and in any case could easily be broken."[113] Encryption was therefore considered a life skill for eighteenth-century statesmen. Indeed, many were quite open about their privacy concerns and demanded that the recipient either encrypt their reply or delay further discussion until the parties could meet in person.

The Founders' own letters reveal deep concern about postal insecurity. Jefferson wrote candidly about such worries, writing to an ally: "I owe you a political letter. yet [sic] the infidelities of the post office and the circumstances of the times are against my writing fully & freely."[114] Likewise, Washington wrote in a letter to his friend the Marquis de Lafayette after the Revolutionary War that his "sentiments with respect to the merits of the new Constitution . . . [b]y passing through the Post offices . . . should become known to all the world."[115] Many Americans at the Founding are recorded to have shared their concern. Indeed, "the diaries and correspondence of early Americans are filled with veiled (or not so veiled) references to the insecurity of the postal system, and the use of codes and ciphers was commonplace."[116]

---

[111] *See* WEBER, *supra* note 45, at 15 ("Enciphered letters, in and of themselves, were not as suspicious then as they would be today.").

[112] *See id.* ("Personal correspondence was often enciphered for everyday privacy purposes.").

[113] Desai, *supra* note 79, at 562 ("This was in an era long before the envelope . . . .").

[114] Letter from Thomas Jefferson to John Taylor (Nov. 26, 1798), *in* 30 THE PAPERS OF THOMAS JEFFERSON 588–90 (Barbara B. Oberg ed., 2003) (Jefferson's original capitalization and punctuation retained).

[115] Letter from George Washington to the Marquis de Lafayette (Feb. 7, 1788), *in* 6 THE PAPERS OF GEORGE WASHINGTON, CONFEDERATION SERIES 95–98 (W. W. Abbot ed., 1977).

[116] FREDERICK S. LANE, AMERICAN PRIVACY: THE 400-YEAR HISTORY OF OUR MOST CONTESTED RIGHT 8 (2009).

Concerns over postal insecurity had been mounting since the Colonial era; many early Americans harbored an instinctive distrust of British control over what was then known as the "Parliamentary Post."[117] In fact, as early as 1742, self-censorship can be observed in archival records. In one example, emblematic of its time, a Boston physician wrote to his friend: "I'll say no more on this head, but When I have the Pleasure to See you again, shall Inform you of many Things too tedious for a Letter and which perhaps may fall into Ill hands."[118]

As historians have noted, the Founders' concern for the confidentiality of their postal mail was, in retrospect, well founded. By the early 1770s, American leaders "had good reason to worry, that loyalist postmasters would intercept and read their letters, a frightening prospect when much of what they were doing likely constituted treason" to the British.[119]

One Founder in particular played an outsized role in advancing the security of early American postal mail and the revolutionary cause generally: Benjamin Franklin.[120] Although the British government retained control over the colonial postal system pursuant to the Post Office Act of 1710, the Crown maintained a practice of appointing colonists to handle ministerial postmaster roles as "running governmental institutions entirely from England was obviously impractical."[121] Franklin first secured a role as Postmaster of Philadelphia in

---

[117] Desai, *supra* note 79, at 564 (noting that the British post office was more commonly known as the "parliamentary post" in the Founding era).

[118] LANE, *supra* note 116, at 8 (quoting a 1742 letter from Dr. Oliver Noyes to his friend David Jeffries).

[119] Desai, *supra* note 79, at 564 (noting widespread concerns among late-eighteenth-century Americans that loyalist postmasters "would intercept and destroy materials they viewed as seditious" before declaring the author "a 'traitor' to the British").

[120] Franklin initially took on a postmaster role for business reasons. As a struggling printer and newspaper publisher, he stood to gain from the fringe benefits of securing a postmaster appointment. The accompanying so-called "franking" privileges allowed Franklin to mail his newspaper, *The Pennsylvania Gazette*, to readers at no cost. DEVIN LEONARD, NEITHER SNOW NOR RAIN: A HISTORY OF THE UNITED STATES POSTAL SERVICE 4 (2016). Although the direct compensation—a ten percent commission on senders' postage—did not amount to much at the time, this fringe benefit would ultimately allow Franklin to grow the circulation of *The Pennsylvania Gazette* into one of the colonies' most successful newspapers. *See id.* at 2–3. In his *Autobiography*, Franklin later conceded that his appointment as Postmaster of Philadelphia was a considerable boon to his publishing business: "Though the salary was small, it facilitated the correspondence that improved my newspaper, increased the number demanded, as well as the advertisements to be inserted, so that it came to afford me a considerable income." LANE, *supra* note 116, at 7.

[121] LANE, *supra* note 116, at 19; *see also* Post Office Act, 1710, 9 Ann., c. 10, § 4 (authorizing postmaster general to appoint deputies at offices in American colonies and West Indies).

1737.[122] British authorities were reportedly impressed with his rather meticulous record keeping, as his predecessor had been removed for failing to submit timely postal ledgers.[123]

Franklin went on to secure a promotion to Deputy Postmaster General of British America in 1753.[124] Although Franklin nominally shared the appointment with a Virginia-based planter by the name of William Hunter, historians note that Franklin took the leading role.[125] During his twenty-one-year tenure as Deputy Postmaster General for the colonies, Franklin orchestrated considerable reforms, including several designed to boost the security of mailed letters. For example, he required that all post office employees take the following oath vowing not to tamper with the letters under their care: I "do swear, That I will not wittingly, willingly, or knowingly open . . . or cause, procure, permit, or suffer to be opened . . . any Letter or Letters . . . which shall come into my Hands, Power, or Custody, by Reason of my Employment in or relating to the Post Office; except . . . by an express Warrant in Writing under the Hand of one of the principal Secretaries of State for that purpose."[126]

He also, among other changes, required local postmasters scattered across the colonies "to keep their post offices separate and apart from their homes and to make sure that no unauthorized individuals handled the mail . . . to seal the mail for each town in a bag . . . to unseal the mail bag only when they reached the destination town . . . and to request proof of identification before allowing someone to retrieve a posted letter."[127]

Separately from these privacy-enhancing operational improvements, Franklin encouraged Americans—particularly young men who sought to enter business or advance their position in society—to learn encryption. In fact, he published a guide written for young men advising them to encrypt their

---

[122] LANE, *supra* note 116, at 7 ("On October 27, 1737, an announcement appeared in the Pennsylvania Gazette, a newspaper published by a struggling printer named Benjamin Franklin, declaring that he was now the operator of 'the Post-Office of Philadelphia.'").

[123] LEONARD, *supra* note 120, at 3 (explaining that the British removed Franklin's predecessor "because he had neglected to submit his financial reports for three years in a row").

[124] *See* LANE, *supra* note 116, at 7.

[125] *See* LEONARD, *supra* note 120, at 5 ("[T]he amiable Hunter generally deferred to Franklin so the arrangement worked well. Now Franklin had his chance to reconceive the colonial post.").

[126] DAVID H. FLAHERTY, PRIVACY IN COLONIAL NEW ENGLAND 121 (1972).

[127] LANE, *supra* note 116, at 8.

sensitive letters and providing instructions on how to do so via the use of codes and ciphers.[128]

The guide was based on "a popular manual of English grammar, penmanship, composition, arithmetic, bookkeeping, and other useful matters for young men entering business" written originally by an Englishman.[129] Franklin changed the title to "The American Instructor" and omitted some parts of the British edition while adding "new material for American readers," such as "accounts of the history and government of the several colonies."[130] Included in the guide were instructions on how to deploy twelve different cipher algorithms to encrypt letters.[131]

As Franklin well knew, those who did not encrypt their letters faced the risk of having their personal secrets exposed or even leaked to the press in a scandal. One such scandal that gripped the colonies, drawing revolutionary fervor and fueling calls for American independence, was that of Massachusetts Governor Thomas Hutchinson. A series of private letters between Governor Hutchinson and his deputy were leaked and published by newspapers across the colonies.[132] In the leaked letters, Governor Hutchinson reportedly stated that Americans were owed fewer rights and privileges than English citizens.[133] Americans were infuriated by these statements, and some took to burning effigies of Governor Hutchinson.[134]

---

[128] The guide also provided advice on accounting, carpentry, and dye-mixing, among other life skills for the Colonial era. *See* FISHER, *supra* note 46, at iii–v. Franklin's publication was one of many guides to encryption in circulation at the time. *See, e.g.*, JOHANN JACOB WECKER, DE SECRETIS, LIBRI XVII (1582); FRANCIS BACON, THE TWOO BOOKES OF FRANCIS BACON 1.61 (1605) (providing instructions for the use of ciphers); SIR SAMUEL MORLAND, A NEW METHOD OF CRYPTOGRAPHY (1666); JOHN FALCONER, CRYPTOMENYSIS PATEFACTA; OR THE ART OF SECRET INFORMATION (1685); JOHN DAVYS, AN ESSAY ON THE ART OF DECYPHERING (1737); PHILIP THICKNESSE, A TREATISE ON THE ART OF DECYPHERING (1772).

[129] Advice to a Young Tradesman (July 21, 1748), *supra* note 46.

[130] *Id.* (explaining that the guide was "[a] competitor of William Mather's *The Young Man's Companion*, on which it was based and from which it copied many particulars").

[131] *Id.* (noting that these encryption techniques were designed by Franklin's late friend Joseph Breintnall). Franklin apparently took some pride in its publication, referring to the guide he published as the "little piece of mine" in a letter to his cousin. Letter from Benjamin Franklin to Samuel Franklin (July 7, 1773), *supra* note 46.

[132] *See* RUSS CASTRONOVO, PROPAGANDA 1776: SECRETS, LEAKS, AND REVOLUTIONARY COMMUNICATIONS IN EARLY AMERICA 46 (2014) (noting that leaked letters consisted of "a packet of correspondence to England" in which Hutchinson "laid out his take on American affairs").

[133] *See id.* at 46, 65 (observing that Hutchinson's letter book stipulated: "I consider this a private letter . . . and wish it may go no further").

[134] *See* H.W. BRANDS, THE FIRST AMERICAN: THE LIFE AND TIMES OF BENJAMIN FRANKLIN 459–60, 484 (2010).

Months later, on Christmas Day in 1773, Franklin published a "Public Statement about the Hutchinson Letters," admitting that he had, in fact, been the source of the leak. The scandal, as expected, led to the loss of his appointment as Deputy Postmaster General of British America.[135] The nation, however, soon erupted into war, and Franklin would subsequently be appointed the first Postmaster General of the United States by the Continental Congress.

B. Insistence on Encrypted Communications Was Pervasive Among the Founders and Founding-Era Presidents

Franklin's publication of a guide to encryption may have been unique among the Founders, but his insistence on encrypted communication was certainly not.[136] In the years after the fledgling nation reached peace with Britain, historical records indicate that letters, including those sealed in wax, continued to be intercepted with concerning regularity.[137] Both Washington and Jefferson, for instance, "complained bitterly about their mail being opened and read in the post-war era."[138]

Madison's correspondence demonstrates that he appreciated the reality of the situation and, in response, endeavored to encrypt sensitive letters. As he wrote to Jefferson in 1784: "My two last [letters], neither of which were in cypher, were written as will be all future ones in the same situation, in expectation of their being read by the postmasters. I am well assured that this

---

[135] Franklin's Public Statement about the Hutchinson Letters (Dec. 25, 1773), *in* 20 THE PAPERS OF BENJAMIN FRANKLIN 513–16 (William B. Willcox ed., 1976) (observing that Franklin's statement "received wide publicity in America" and "touched off a virulent newspaper campaign against him" in Britain).

[136] *See, e.g.*, Letter from William Carmichael to Benjamin Franklin (Jan. 25, 1780), *in* 31 THE PAPERS OF BENJAMIN FRANKLIN 406–08 (Barbara B. Oberg ed., 1995) ("I write at the same time to Dr. Bancroft who will communicate in Cypher any thing that you may think improper to trust to the Common Conveyance."); *see also* WEBER, *supra* note 45, at xi ("[T]he Founding Fathers quickly, though sometimes inexpertly, recognized the dire necessity for more secure communications."); RALPH E. WEBER, UNITED STATES DIPLOMATIC CODES AND CIPHERS, 1775-1938, at 118 (1979) ("A new American government under the Constitution began in 1789 with several revolutionary figures filling the most crucial posts . . . . Most of them were well acquainted with codes and ciphers.").

[137] *See* DAVID J. SEIPP, THE RIGHT TO PRIVACY IN AMERICAN HISTORY 1, 11 (1978); LEONARD D. WHITE, THE FEDERALISTS: A STUDY IN ADMINISTRATIVE HISTORY 191 (1956); *cf.* WILCOX, *supra* note 76, at 46 ("Hard-fought independence from Britain was achieved with the help of codes, ciphers, invisible ink, visual communications, and hidden messages.").

[138] Desai, *supra* note 79, at 565; *see also* Kerr, *supra* note 5, at 917 (discussing the "the insecurity of postal letters" in "the eighteenth and nineteenth centuries").

is the fate of all letters . . . . Having now the use of my cypher I can write without restraint."[139] Jefferson echoed the insistence on encryption to others, including in his correspondence with Founder Robert Livingston: "[W]hy a cypher between us . . . . [T]here may be matters merely personal to ourselves, and which require the cover of a cypher . . . . This last purpose . . . may render it convenient & advantageous to have at hand a mask for whatever may need it."[140]

In his earlier years, Washington demonstrated a penchant for invisible ink rather than encryption, as the latter could prove cumbersome at times.[141] Washington procured what he referred to as "white ink" from Sir James Jay, a London physician and brother of future Chief Justice Jay.[142] Sir Jay had invented a chemical composition that appeared virtually invisible to the eye but could be made visible by wetting the paper with a brush soaked in a second chemical. Sir Jay sent phials of both liquids—the invisible ink and the accompanying revealing ink—to his brother John as well as to Washington.[143]

---

[139] Letter from James Madison to Thomas Jefferson (Oct. 17, 1784), *in* 8 THE PAPERS OF JAMES MADISON 118–22 (Robert A. Rutland & William M. E. Rachal eds., 1973).

[140] Letter from Thomas Jefferson to Robert Livingston (Apr. 18, 1802), *in* 37 THE PAPERS OF THOMAS JEFFERSON, *supra* note 45, at 263–67; *cf.* Letter from Thomas Jefferson to James Madison (Aug. 18, 1803), *in* 5 THE PAPERS OF JAMES MADISON, SECRETARY OF STATE SERIES 323–25 (David B. Mattern et al. eds., 2000) ("I inclose you two letters from Rob. R. Livingston. That of the 2d. of June is just intelligible enough in the uncyphered parts to create anxieties which perhaps the cypher may remove. I communicate them for your information, & shall be glad to recieve [sic] them decyphered.").

[141] This Article's analysis of encrypted correspondence notably cannot include the private letters between George and Martha Washington, as Martha Washington deliberately destroyed nearly all of their correspondence following her husband's death in 1799. Of the thousands of letters they presumably exchanged during their 40-year marriage and George Washington's extensive public service, only a handful of letters between them survive. *See* Letter from George Washington to Martha Washington (June 18, 1775), *in* 1 THE PAPERS OF GEORGE WASHINGTON 3–6 (Philander D. Chase ed., 1985). Martha Washington's systematic destruction of their correspondence was a common practice among prominent families of the era seeking to protect their privacy, though it has created an irreparable gap in the historical record. While George Washington's preserved papers contain extensive encrypted diplomatic and military correspondence, the loss of his private letters with Martha precludes any analysis of whether the Washingtons employed encryption methods in their personal communication during his extended absences leading the Continental Army or serving as the nation's first president. This absence in the historical record is particularly noteworthy given Washington's documented use of encryption in both military dispatches and sensitive political correspondence with other Founders discussed in this Article. *See* Letter from George Washington to the Marquis de Lafayette, *supra* note 115; *infra* notes 145–147.

[142] *See* WEBER, *supra* note 45, at 44.

[143] *See id.* (explaining that the "use of secret fluids dates back to antiquity").

In the years after the war, Washington transitioned to encrypted writing rather than invisible ink. His reason for the shift is lost to time—he is recorded to have told associates to "economize in writing with the special ink because he had only small amounts" and, therefore, may have run out.[144] Alternatively, perhaps Washington believed that the invisible ink methodology had been compromised and therefore could no longer be relied upon to ensure confidentiality in a newly independent America.

A number of Washington's letters dating from September 12, 1780, onward deploy encryption or otherwise refer to his preference for ciphered messages. [145] Perhaps most illuminating is Washington's encrypted correspondence with Henry Innes. After the Constitution was ratified, but before Washington assumed the presidency, Innes wrote to Washington seeking his aid in opposing Kentucky leaders who had been contemplating secession.[146] Rather than respond openly as the soon-to-be leader of the newly formed republic, Washington insisted that his support be kept strictly confidential, promising to send Innes a "cypher" to encrypt their correspondence.[147]

---

[144] *Id.* (noting the usefulness of invisible ink for letters sent to or from New York as British troops were opening such letters).

[145] *See*, *e.g.*, Letter from George Washington to Rear Admiral Guichen (Sep. 12, 1780), *in* 28 THE PAPERS OF GEORGE WASHINGTON, REVOLUTIONARY WAR SERIES 181–84 (William M. Ferraro & Jeffrey L. Zvengrowski eds., 2020) ("I have no cypher of communication with the Count[.] I take the liberty to request Your Excellency's assistance in making use of yours and forwarding it by triplicates with your dispatches by the first opportunities."); Letter from George Washington to the Marquis de Lafayette (Sep. 1, 1785), *in* 3 THE PAPERS OF GEORGE WASHINGTON, CONFEDERATION SERIES 215–18 (W. W. Abbot ed., 1994) ("Since my last to you, I have been favored with your letters of the 11th & 13th of May by young Mr Adams, who brought them to New York, from whence they came safely to this place by the Post: the first is in Cypher; & for the communications therein contained I thank you."); Letter from William Gordon to George Washington (Feb. 16, 1786), *in* 3 THE PAPERS OF GEORGE WASHINGTON, CONFEDERATION SERIES, *supra* note 145145, at 559–60 ("Have drawn out the cypher (which I shall enclose) & given a specimen of the mode of working with it.").

[146] *See* Letter from Harry Innes to George Washington (Dec. 18, 1788), in 1 THE PAPERS OF GEORGE WASHINGTON, PRESIDENTIAL SERIES 187–90 (Dorothy Twohig ed., 1987) (suggesting that Washington "invent a Cypher" to protect the secrecy of their correspondence); *id.* at 189 n.1 (editor's note explaining that "Spanish and British agents . . . were attempting to woo Kentucky leaders away from the Confederation government").

[147] *See* Letter from George Washington to Harry Innes (Mar. 2, 1789), *in* 30 THE WRITINGS OF GEORGE WASHINGTON 214–15 (John C. Fitzpatrick ed., 1944). Innes would later serve as the first United States District Judge in Kentucky.

C. The Founders Encrypted Courtship Letters in Addition to Those Communicating Political Activism and Financial Affairs

The letters of the Founders are among the best preserved of late-eighteenth-century American correspondence, thanks in large part to both government and private support for their preservation.[148] These preserved letters demonstrate that Washington was not alone in his reliance on encrypted messages. A broad range of Founders, including the first five Presidents of the United States, deployed encryption in their private capacities, both before and after the Revolutionary War.[149]

Their use of encrypted communication extended beyond politics and business to matters of the heart as well. In one early example, Jefferson encrypted his correspondence with college friend John Page "regarding a young lady he was courting," Rebecca Burwell.[150] Jefferson had previously "disguised her name by referring to her as 'R.B.,' 'Belinda,' 'Adnileb,' and 'Campana in die,'" but the young Jefferson grew concerned that these pseudonyms could nevertheless expose their courtship.[151] Jefferson insisted that the pair use an old English book to encode their correspondence.[152]

---

[148] For discussion of the systematic preservation efforts that have made the Founders' papers uniquely accessible to historians, see Williams, *supra* note 106 (describing the National Historical Publications and Records Commission's decades-long funding of documentary editions of the Founders' papers, which have produced "literally hundreds of thousands of linear feet of archival material"). While these extensive collections allow us to trace encryption practices among political elites, the relative scarcity of preserved correspondence from other segments of early American society means we have a more limited understanding of how encryption may have been used in broader communication networks.

[149] *See, e.g.*, WEBER, *supra* note 45, at xiii ("And 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."); Letter from James Monroe to James Madison (Nov. 15, 1784), *in* 8 THE PAPERS OF JAMES MADISON 140–43 (Robert A. Rutland & William M. E. Rachal eds., 1973) ("You rec[eive]d I hope by the last post a small cypher from me.").

[150] WEBER, *supra* note 45, at 39 (quoting Jefferson: "We must fall on some scheme of communicating our thoughts to each other, which shall be totally unintelligible to every one but to ourselves.").

[151] *Id.*; *see, e.g.*, Thomas Jefferson to John Page (Jan. 20, 1763), *in* 1 THE PAPERS OF THOMAS JEFFERSON 7–9 (Julian P. Boyd ed., 1950) ("How does R. B. do? . . . For you must know that as soon [as t]he Rebecca (the name [I] intend to give the vessel above mentioned) is completely finished I intend to hoist sail and away.").

[152] WEBER, *supra* note 45, at 39 (noting "Jefferson's anxieties about keeping his correspondence entirely private"); Thomas Jefferson to John Page (Jan. 23, 1764), in 1 THE PAPERS OF THOMAS JEFFERSON, supra note 151, at 14–15 (Julian P. Boyd ed., 1950) ("We must fall on some scheme of communicating our thoughts to each other, which shall be totally

Madison's courtship of Catherine 'Kitty' Floyd offers another example. He encoded letters confessing his feelings for Floyd, the daughter of a New York delegate to the Continental Congress who would at one point become his fiancée before ultimately breaking off the engagement.[153] In yet another instance, Jefferson wrote to John Adams with an encrypted message for his daughter concerning "a young gentleman of her acquaintance who has a very sincere and high affection for her."[154] Jefferson indicated that "the following paragraphs are for her eye only" and asked Adams to "be so good . . . as to deliver over the letter to her."[155] Jefferson indicated that the potential suitor must have already given her the decryption key when the two had met in person.[156]

D. The Founders' Insistence on Encryption Persisted Despite Inevitable Frustrations and the Likelihood of Errors

The Founders' reliance on encryption—despite its frustrations and frequent technical failures—offers powerful evidence that they regarded the confidentiality of communication as vital to expression. Archival records show that leaders across the early republic persisted through the tedium of ciphers and codes because they understood encryption not as convenience, but as essential to securing their private correspondence.

This was no mere intellectual diversion or demonstration of cryptographic prowess. Rather, the historical record shows that the Founders devoted substantial time and effort to encryption despite its tedious nature and high error rate. Their letters document frequent struggles with complex cipher systems, mistakes in encoding and decoding messages, and the frustration of failed communication attempts. Yet rather than abandon encryption in the face

---

unintelligible to every one but to ourselves. I will send you some of these days Shelton's Tachygraphical Alphabet, and directions.").

[153] *See*, *e.g.*, Letter from Thomas Jefferson to James Madison (Apr. 14, 1783), *in* 6 THE PAPERS OF THOMAS JEFFERSON 261–62 (Julian P. Boyd ed., 1952) ("Be pleased to make my compliments affectionately to the gentlemen and ladies. I desire them to Miss Kitty particularly."); RALPH LOUIS KETCHAM, JAMES MADISON: A BIOGRAPHY 108–11 (1990) ("For reasons unknown, she decided to break her engagement to Madison . . . She wrote Madison a letter in July 1783, containing . . . a 'profession of indifference,' and sealed it, according to Floyd family tradition, with a piece of rye dough.").

[154] Letter from Thomas Jefferson to John Adams (June 2, 1785), *in* 17 THE ADAMS PAPERS, PAPERS OF JOHN ADAMS 145–47 (Gregg L. Lint et al. eds., 2014).

[155] *Id.*

[156] *See id.* ("[T]he cypher I suppose to be in her custody.").

of these challenges, they persisted in developing and refining their methods. When one system proved too cumbersome or error-prone, they worked to devise more reliable alternatives.

The archival records, for example, suggest that Adams, in his own correspondence, struggled and at times grew frustrated with the lengthy decryption process. As Adams confessed to friend Arthur Lee in 1779, "I am no Hand at a Cypher, but will endeavour, to unridel if you write in it."[157] Encrypting only portions of the messages, particularly sensitive sentences or paragraphs, lessened the burden imposed on both the author and the letter's recipient, who would ultimately be tasked with decrypting the amalgamation of characters.

The potential for user error in the decryption process was not lost on the Founders.[158] Many, like Adams, sometimes expressed frustration and made mistakes in encrypting letters. Madison, for example, in a 1783 letter to Edmund Randolph conceded, "The tediousness of the Cypher does not permit me now to enter into detail."[159] In another letter to Randolph, Madison complained that, "I wish we could somehow or other substitute a more convenient" cipher, lamenting that "great caution is necessary to avoid errors" with the current one.[160] The archivists who decrypted Madison's letters centuries later called Madison's frustration "well justified" as the code that the pair previously deployed comprised more than six hundred different numerals.[161] In other instances, however, the encryption errors were, in fairness, Madison's mistake. Once, he sent a cipher with only twenty-four letters in the alphabet rather than the expected twenty-six.[162]

---

[157] Letter from John Adams to Arthur Lee (Mar. 24, 1779), in 8 THE ADAMS PAPERS, PAPERS OF JOHN ADAMS 16–17 (Gregg L. Lint et al. eds., 1989); see also Letter from Arthur Lee to John Adams (Mar. 18, 1779), *in* 8 THE ADAMS PAPERS, PAPERS OF JOHN ADAMS, *supra* note 157, at 12–13 ("[A]ll my Letters have been open[e]d at the Post . . . . Will you send me a Cypher, or shall I make one for the greater Security in writing?").

[158] *See*, *e.g.*, Letter from Thomas Jefferson to James Madison (Feb. 14, 1783), *in* 6 THE PAPERS OF THOMAS JEFFERSON, *supra* note 153, at 241–44 ("I am very particularly indebted here to the politeness and hospitality of Genl. La Vallette who obliges me to take refuge in his quarters from the tedium of my own, the latter half of every day. You are indebted to him too as I should make my long letters much longer and plague you with more cypher were I confined at home all day.").

[159] Letter from James Madison to Edmund Randolph (Mar. 18, 1783), *in* 6 THE PAPERS OF JAMES MADISON, *supra* note 47, at 354–57.

[160] Letter from James Madison to Edmund Randolph (Feb. 4, 1783), *in* 6 THE PAPERS OF JAMES MADISON, *supra* note 47, at 193–94.

[161] *Id.*

[162] Letter from Philip Mazzei to James Madison (June 13, 1779), *in* 1 THE PAPERS OF JAMES MADISON 284–87 (William T. Hutchinson & William M. E. Rachal eds., 1962).

Jefferson and Madison reportedly encountered some difficulties when corresponding with each other via encrypted letters in the early 1780s. The code system that they deployed "proved complicated and frustrating as Madison had considerable difficulty decoding Jefferson's letters, often miscounting the lines, or misunderstanding Jefferson's choice of numbers."[163] The two subsequently switched encryption methods to a more sophisticated variant that "while not error-proof, did eliminate the common error of miscounting lines and word positions."[164]

Franklin, in another example, admitted that, "The Cypher you have communicated, either from some Defect in your Explanation or in my Comprehension, is not yet of use to me" and suggested instead that his counterpart deploy a simpler cipher that they use "when a few Sentences only are required to be writ in Cypher" as "it is too tedious for a whole Letter."[165] As it turns out, the error was not Franklin's.[166] His counterpart had mistakenly written "13" instead of "1," which explains his confusion.[167] Franklin's private papers show that he tried to write out every possible permutation of letters for the erroneous sentence but ultimately was not successful in decrypting it—hence, the quite understandable frustration on his part.[168]

Archival records indicate that Jefferson also struggled at times with the encryption process. For example, in a 1784 letter to fellow Virginian and future President James Monroe, Jefferson wrote, "[I] could not there make out the passages which were put into cypher. I have tried it here and find that by some unfortunate mistake, probably in the young gentleman who wrote the cypher,

---

[163] WEBER, *supra* note 136, at 118.

[164] *Id.* (noting that "the Jefferson-Madison correspondence left a wake of garbled messages for future editors to translate into plaintext").

[165] Letter from Benjamin Franklin to James Lovell (Aug. 10, 1780), *in* 33 THE PAPERS OF BENJAMIN FRANKLIN 169–71 (Barbara B. Oberg ed., 1997).

[166] *See* Letter from James Lovell to Benjamin Franklin (May 4, 1780), *in* 32 THE PAPERS OF BENJAMIN FRANKLIN 354–55 (Barbara B. Oberg ed., 1996), at n.2 (noting Franklin "became confused at number 13 (which was Lovell's mistake, it ought to have been a 1)"); *cf.* Letter from Benjamin Franklin to James Lovell (Feb. 24, 1780), *in* 31 THE PAPERS OF BENJAMIN FRANKLIN 520–22 (Barbara B. Oberg ed., 1980) ("Lovell was exceptionally obscure in his cipher explanations . . . . The unfortunate result was that they even defied Benjamin Franklin's attempts to understand them.").

[167] Letter from James Lovell to Benjamin Franklin (May 4, 1780), *in* 32 THE PAPERS OF BENJAMIN FRANKLIN, *supra* note 166, at 354–55 ("Lovell sent John Adams an explanation of the cipher in a letter of this same date, but John Adams had no more luck with it than did Benjamin Franklin.").

[168] *See id.* at n.2.

it will not explain a single syllable."[169] Jefferson followed up with Monroe a few months later after identifying Monroe had, in fact, used the wrong cipher, which created the confusion: "[Y]our letters [t]hose of Nov. 1 and Dec. 14 having rendered me extremely desirous of decyphering them, I sat to work with a resolution to effect it if possible. I soon found that they were written by your first cypher. To this therefore I applied myself and after several days spent on it I was able to set to rights the many errors of your copyist, whose inattention alone had induced those difficulties."[170]

Going back and forth over encryption errors was not uncommon at the time. The process, even with the assistance of clerks, was subject to user error. In a 1788 letter, Jefferson documents some of his encryption struggles: "The cyphered words in your letter of Apr. 14 prove to me that Mr. Barclay left you a wrong cypher. In those of May 8, taken from the cypher I sent you, are several things which I cannot make out."[171]

Jefferson usually persisted in his insistence on encrypting communications, notwithstanding the risk of error: "I cite the following passage, drawing lines under the numbers I do not understand. '1001. 739. 1264. 1010. 1401. 1508. 1237. 1509. 950. 1509. 694. 861. 221. 742. 658. 233. 1017. 1077. 1097.' and I do it that we may come to a perfect understanding of our cypher."[172] In a few instances, however, Jefferson relented and sent information in unencrypted form—albeit shrouded in ambiguity that would hopefully render the communication unintelligible to third parties. A 1784 letter preserved in his private papers offers one such example: "For fear you should not understand the cypher, or catch its key I added that ænigmatical paragraph in hopes it

---

[169] Letter from Thomas Jefferson to James Monroe (Nov. 11, 1784), *in* 7 THE PAPERS OF THOMAS JEFFERSON 508–14 (Julian P. Boyd ed., 1953) ("The want of the cypher would have restrained me from mentioning some things were I not assured of the fidelity of the bearer hereof Colo. Le Maire.").

[170] Letter from Thomas Jefferson to James Monroe (Feb. 6, 1785), *in* 7 THE PAPERS OF THOMAS JEFFERSON, *supra* note 169, at 637–41 ("Since writing so far I have made out a table adjusting the numbers in my copy to those in yours, which will enable you to translate with ease.").

[171] Letter from Thomas Jefferson to William Carmichael (June 3, 1788), *in* 13 THE PAPERS OF THOMAS JEFFERSON 229–35 (Julian P. Boyd ed., 1956).

[172] *Id.* ("I suppose some of these to have been intended, others I ascribe to the equivocal hand writing in the cypher, which I believe was by one of Mr. Barclay's clerks. I cannot always distinguish the letter e. from o. n. from u. t. from f. and sometimes from s. I observe you use repeatedly 1360. instead of 1363. which I presume to be an error of the copyist to be corrected in your cypher.").

might explain a subject to you who had some hint of it and not to any other who had not."[173]

The Founders' willingness to labor over encryption—spending days deciphering garbled messages or trading letters to correct a single error—shows that they regarded secure communication as far more than an intellectual curiosity. Their persistence, even in the face of frustration, reveals a conviction that privacy was not a luxury but a necessity: an essential instrument for protecting candor in correspondence, worth the effort it demanded.

E. Madison and Jefferson Debated the First Amendment's Text via Encrypted Letters

In debates over whether encryption falls within the First Amendment's scope, a remarkable historical parallel has gone largely unnoticed: the very text of the First Amendment was debated and refined through encrypted correspondence between Madison and Jefferson. This episode is more than a historical curiosity; it reveals that the Framers themselves grasped the connection between secure private communication and the free exchange of ideas that the Amendment safeguards.

Although Jefferson at the time sat more than three thousand miles away in Paris while Americans debated the merits of the amendments that Madison proposed, he remained in continued contact with Madison, a fellow Virginian and lifelong friend.[174] Their correspondence over this period is interspersed with encrypted sentences and paragraphs, as the two sought to keep their plans and drafting confidential. Philadelphia hosted the Constitutional Convention in the summer of 1787. Jefferson, however, had been in France since 1785, when he succeeded Franklin as the nation's ambassador. Jefferson received partially encrypted updates from Madison on the Convention's progress, including a list of the individuals attending[175] as well as details on key provisions that were going to be included in the Constitution.[176] Madison sent a copy of the newly

---

[173] Letter from Thomas Jefferson to William Short (Mar. 1, 1784), *in* 6 THE PAPERS OF THOMAS JEFFERSON, *supra* note 153, at 569–70.

[174] *See* Lawrence S. Kaplan, *Jefferson and the Constitution: The View from Paris, 1786–89*, 11 DIPLOMATIC HIST. 321, 321 (1987); *infra* notes 177–189.

[175] *See* Letter from James Madison to Thomas Jefferson (June 6, 1787), *in* 11 THE PAPERS OF THOMAS JEFFERSON 400–02 (Julian P. Boyd ed., 1955) ("The members present are . . . .").

[176] Letter from James Madison to Thomas Jefferson (Sep. 6, 1787), *in* 10 THE PAPERS OF JAMES

signed Constitution to Jefferson in October 1787, after which Jefferson responded with cajoling encouragement, prodding Madison to get to work on an accompanying bill of rights.[177]

Their use of partial encryption for sensitive portions of these letters allowed the pair to express candid reactions to the document, as well as to the ongoing ratification debates, in a way that plain text may not have allowed. As Jefferson wrote in his December 1787 reply to Madison, offering his initial thoughts after review of the nascent Constitution: "I have much to thank you for. First and most for the cyphered paragraph respecting myself. These little informations are very material towards forming my own decisions."[178]

Jefferson's partially encrypted letter also included a discussion of what he disliked: first and foremost, "the omission of a bill of rights" enumerating what he saw as the fundamental guarantees of "freedom of religion, freedom of the press, protection against standing armies, restriction against monopolies, the eternal and unremitting force of the habeas corpus law, and trials by jury."[179]

The records of their correspondence indicate that Jefferson did not relent in his insistence on a bill of rights, even as Madison shifted his attention to ensuring the ratification of the Convention's Constitution. Madison, for his part, replied in earnest, offering to work with Jefferson on a draft: "My own opinion has always been in favor of a bill of rights; provided it be so framed as not to imply powers not meant to be included in the enumeration. At the same time I have never thought the omission a material defect, nor been anxious to supply it even by subsequent amendment, for any other reason than that it is anxiously desired by others. I have favored it because I supposed it might be of use, and if properly executed could not be of disservice."[180]

MADISON 163–65 (Robert A. Rutland et al. eds., 1977).

[177] Letter from James Madison to Thomas Jefferson (Oct. 24, 1787), *in* 10 THE PAPERS OF JAMES MADISON, *supra* note 176, at 205–20 ("You will herewith receive the result of the Convention, which continued its Session till the 17th. of September. I take the liberty of making some observations on the subject which will help to make up a letter, if they should answer no other purpose."); Letter from Thomas Jefferson to James Madison (Dec. 20, 1787), *in* 10 THE PAPERS OF JAMES MADISON, *supra* note 176, at 335–39.

[178] Letter from Thomas Jefferson to James Madison (Dec. 20, 1787), *supra* note 177.

[179] *Id.*

[180] Letter from James Madison to Thomas Jefferson (Oct. 17, 1788), *in* 11 THE PAPERS OF JAMES MADISON 295–300 (Robert A. Rutland & Charles F. Hobson eds., 1977) ("[A] bill of rights can serve an important educational function, reminding the people of their most cherished liberties; plus, it can also provide the people with a set of criteria to use when criticizing the government for its abuses.").

By 1789, Jefferson's advocacy for a bill of rights became even more insistent. On March 15, he wrote Madison, "In the arguments in favor of a declaration of rights, you omit one which has great weight with me, the legal check which it puts into the hands of the judiciary."[181] He pleaded, "Half a loaf is better than no bread. If we cannot secure all our rights, let us secure what we can."[182]

Madison responded two months later with a partially encrypted letter, updating Jefferson on the progress of the proposed amendments and explaining that "[t]he subject of amendments was to have been introduced on monday last; but is postponed in order that more urgent business may not be delayed."[183] Archival records show that Jefferson decrypted Madison's letter "interlinearly"—in other words, his handwriting appears between the lines of Madison's encrypted text with the letter's deciphered meaning.[184] On June 30, Madison followed through, enclosing the actual text of his proposed amendments and noting that he had "studiously avoided" anything "of a controvertible nature that might endanger the concurrence of two-thirds of each House and three-fourths of the States."[185]

Jefferson responded in kind with his own partially encrypted letter. He commented favorably on Madison's draft but proposed his own, even stronger, language clarifying those rights he found fundamental:

> I must now say a word on the declaration of rights you have been so good as to send me. I like it as far as it goes; but I should have been for going further. For instance the following alterations and additions would have pleased me.
>
> Art. 4. The people shall not be deprived or abridged of their right to speak to write or otherwise to publish any thing but false facts affecting

---

[181] Letter from Thomas Jefferson to James Madison (Mar. 15, 1789), *in* 14 THE PAPERS OF THOMAS JEFFERSON 659–63 (Julian P. Boyd ed., 1979).
[182] *Id.*
[183] Letter from James Madison to Thomas Jefferson (May 27, 1789), *in* 12 THE PAPERS OF JAMES MADISON 185–87 (Charles F. Hobson & Robert A. Rutland eds., 1979).
[184] *Id.*
[185] Letter from James Madison to Thomas Jefferson (June 30, 1789), *in* 12 THE PAPERS OF JAMES MADISON, *supra* note 183, at 267.

> injuriously the life, liberty, property, or reputation of others or affecting the peace of the confederacy with foreign nations.[186]

Archivists have confirmed that Madison, by his own hand, decrypted Jefferson's letter using a cipher the pair had employed since May 11, 1785, shortly after Jefferson left for France.[187]

As this correspondence reveals, encryption served as more than mere technological convenience—it enabled the kind of candid debate and refinement of ideas that the First Amendment was ultimately designed to protect. Their use of ciphers allowed them to engage in frank discussion about the proposed Constitution's strengths and weaknesses, including the critical need for explicit protection of fundamental rights.[188]

The irony is unmistakable: the Framers refined the First Amendment through correspondence secured by ciphers. Madison and Jefferson appreciated that candid discussions required secure channels; encryption was the crucible in which their ideas were tested and tempered. Modern efforts to dilute or defeat encryption therefore do more than compromise privacy. They jeopardize the communicative practice that forged the Amendment itself.

F. The Nation's First Chief Justice Maintained a Practice of Encrypting Sensitive Messages

As a leading Founding-era statesman who served on the Supreme Court during the ratification of the Bill of Rights, Chief Justice Jay's consistent and emphatic use of encryption in his correspondence offers unique insight into how the Founding generation viewed the confidentiality of private communications.

Jay became Washington's first appointment to the Supreme Court in September 1789.[189] He would ultimately resign from the Court six years later in

---

[186] Letter from Thomas Jefferson to James Madison (Aug. 28, 1789), *supra* note 47, at 364–69.

[187] Letter from Thomas Jefferson to James Madison (May 11, 1785), *in* 8 THE PAPERS OF THOMAS JEFFERSON 147–48 (Julian P. Boyd ed., 1953) ("Having lately made a cypher on a more convenient plan than the one we have used, I now transmit it to you . . . .").

[188] Letter from Thomas Jefferson to James Madison (Dec. 20, 1787), *in* 10 THE PAPERS OF JAMES MADISON, *supra* note 176, at 335–39 (acknowledging that "cyphered paragraph[s]" were "very material towards forming my own decisions").

[189] WENDELL BIRD, PRESS AND SPEECH UNDER ASSAULT: THE EARLY SUPREME COURT JUSTICES, THE SEDITION ACT OF 1798, AND THE CAMPAIGN AGAINST DISSENT 118–19 (2016).

1795 to serve as Governor of New York.[190] His tenure on the Court accordingly spanned the ratification of the Bill of Rights and may serve as contemporaneous historical evidence.

Jay garnered almost universal recognition in the Founding era as "one of the new nation's leading statesmen" and had previously joined Alexander Hamilton and Madison as co-author of The Federalist Papers, published under a pseudonym during the national debate over the proposed Constitution.[191]

Although many Americans encrypted their correspondence in the Founding era, Jay's rigid insistence on encryption stands out. Jay had previously assisted with the import of "invisible ink" to the colonies, and, as United States Minister to Spain, developed "an intensified interest" in encryption.[192] Jay's letters appear to exhibit a rigid insistence on security, reflecting an apprehension that candid communication might inadvertently slip through without sufficient protection, either because a message was mistakenly sent unencrypted or because the active cipher had been compromised. For example, in one letter, Jay wrote, "You will oblige me by being very regular & circumstantial in your correspondence, and commit nothing of a private nature to paper unless in cypher."[193] In another, Jay expressed concern that the prior cipher had been compromised, "depriv[ing] [him] of an opportunity of communicating some things which [he] would not wish everybody to know."[194] In yet another, Jay similarly expresses concern about candid communication absent strong encryption: "I do not like the Cypher in which I write, and shall therefore defer

---

[190] *See* Letter from John Jay to George Washington (June 29, 1795), in 18 THE PAPERS OF GEORGE WASHINGTON, PRESIDENTIAL SERIES 272, 272 n.1 (Carol S. Ebel ed., 2015) (enclosing formal resignation stating "Having been elected Governor of the State of New York, & the first Day of next month being assigned for my entering on the Execution of that office, it is proper that I should, and therefore I do hereby resign the office of Chief Justice of the United States").

[191] *Id.* at 119 ("Alexander Hamilton characterized Jay as one of three persons prominent in the public eye, as the successor of the actual President of the United States (who at the time was Washington).").

[192] John Jay's Use of Codes and Ciphers, *supra* note 75.

[193] Letter from John Jay to William Carmichael (Jan. 27, 1780), *supra* note 48, at 18–21.

[194] Letter from John Jay to Robert R. Livingston (Dec. 24, 1779), *in* 1 THE SELECTED PAPERS OF JOHN JAY 744 (Elizabeth M. Nuxoll ed., 2010) ("The Cypher I sent you has I fear become useless. It is a Circumstance which I regret . . . ."); *cf.* Letter from Robert R. Livingston to John Jay (Dec. 22, 1779), *in* 1 THE SELECTED PAPERS OF JOHN JAY, *supra* note 194, at 731–33 ("I could wish to settle a cypher with you that I might for the future write with more freedom than I can now dare to do.").

further Particulars."[195] Indeed, this anxiety over open communication is evident throughout archival records of Jay's private papers.[196]

Jay's correspondence also expresses concern about his recipients' caution in deciphering his letters. For example, in a letter to Founder Robert Livingston, Jay included a "P.S." stating: "When you decypher, do it on a separate paper, & not on the Letter—and as you are sometimes a little careless, destroy the paper immediately."[197] Perhaps most telling of Americans at the Founding, the letter includes an accompanying commentary from archivists who deciphered Jay's papers, noting that his enthusiasm for encryption was "shared with many of his contemporaries."[198]

Jay's nearly obsessive attention to encryption—from his early work importing invisible ink to his repeated warnings about sending sensitive information without proper ciphers—demonstrates that encryption was not merely an occasional convenience but rather an essential tool for enabling the kind of candid discourse necessary for democratic deliberation. That such a prominent judicial figure insisted so emphatically on encryption, even in private correspondence, speaks to the close relationship between message security and expressive freedom.

G. Both Proponents and Opponents of the Sedition Act of 1798 Relied on Encryption

If ever there was a moment to regulate encryption, the Sedition Act of 1798 was it. This episode—widely regarded as the nation's first major constitutional crisis over free speech[199]—saw the Adams administration criminalize criticism

---

[195] Letter from John Jay to Samuel Huntington, Pres. of Congress (Mar. 3, 1780), *in* 2 THE SELECTED PAPERS OF JOHN JAY, *supra* note 48, at 49–51.

[196] *See, e.g.*, Letter from Silas Deane to John Jay (Sep. 13, 1780), *in* 2 THE SELECTED PAPERS OF JOHN JAY, *supra* note 48, at 246–47 ("[A]s I know not whether you may have preserved Our Cypher, I dare not be particular on Subjects which you may wish to hear from me upon."); Letter from Robert Morris to John Jay (July 6, 1780), *in* 2 THE SELECTED PAPERS OF JOHN JAY, *supra* note 48, at 195–96 ("I regret that I did not fix a Cypher with you, as the want of it will prevent me from writing (when I do begin) many things I might wish to Communicate."); Letter from Robert R. Livingston to John Jay (Dec. 22, 1779), *in* 1 THE SELECTED PAPERS OF JOHN JAY, *supra* note 194, at 731–33 ("I could wish to settle a cypher with you that I might for the future write with more freedom than I can now dare to do.").

[197] Letter from John Jay to Robert R. Livingston (Oct. 6, 1780), *in* 2 THE SELECTED PAPERS OF JOHN JAY, *supra* note 48, at 286–89.

[198] John Jay's Use of Codes and Ciphers, *supra* note 75.

[199] *See* N.Y. Times Co. v. Sullivan, 376 U.S. 254, 273 (1964) (characterizing the "great controversy over the Sedition Act of 1798" as the moment that "first crystallized a national

of the President, imprison political opponents, and wield federal power to suppress dissent. And yet, through this turmoil, encryption remained untouched. Neither the Sedition Act's text nor the documented prosecutions under it targeted the use of encryption, nor did contemporaneous debates suggest that such authority existed. That silence, during what is widely considered one of the darkest chapters in First Amendment history, speaks volumes. [200] Under the historical framework established in *Brown v. Entertainment Merchants Ass'n*, this non-regulation during a moment of maximal government overreach offers evidence of First Amendment coverage.

The Sedition Act made it a crime, punishable by a $5,000 fine and five years in prison, for Americans to "write, print, utter or publish any false, scandalous and malicious" statement criticizing the government, Congress, or the President.[201] The Act was widely seen as a political attempt by the Federalist Party—led by President Adams alongside Hamilton—to quash dissent, particularly from the nascent Democratic-Republican Party led by Jefferson and Madison.[202] Curiously, while the Act criminalized criticism of the President, it omitted criticism of the Vice President.[203] In other words, those who voiced criticisms of President Adams could be imprisoned, while opponents of Jefferson, Adams' challenger in the upcoming Presidential election, were free to vocalize their critiques.

---

awareness of the central meaning of the First Amendment").

[200] *See, e.g.*, Watts v. United States, 394 U.S. 705, 710 (1969) (Douglas, J., concurring) ("The Alien and Sedition Laws constituted one of our sorriest chapters . . . ."); Keyishian v. Bd. of Regents of the Univ. of the State of N.Y., 385 U.S. 589, 598 (1967) ("Our experience under the Sedition Act of 1798, 1 Stat. 596, taught us that dangers fatal to First Amendment freedoms inhere in the word 'seditious."').

[201] Sedition Act of 1798, ch. 74, § 2, 1 Stat. 596.

[202] *See* Letter from Thomas Jefferson to James Madison (Apr. 26, 1798), *in* 17 THE PAPERS OF JAMES MADISON 120–22 (David B. Mattern et al. eds., 1991) (explaining that the objective of the "sedition bill" is "the suppression of the whig presses"); *see also* WENDELL BIRD, CRIMINAL DISSENT: PROSECUTIONS UNDER THE ALIEN AND SEDITION ACTS OF 1798, at 42 (2020) ("At the end of congressional debates on the sedition bill, [Congressman Albert] Gallatin exclaimed, 'do they not avow that the true object of the law is to enable one party to oppress the other . . . to have the power to punish printers who may publish against them?' The primary purpose of the Sedition Act was nothing less than to 'try to eliminate the opposition.'").

[203] *See* Sedition Act of 1798, *supra* note 201(criminalizing "writings against the government of the United States, or either house of the Congress, or the President"); *see also* AKHIL REED AMAR, THE BILL OF RIGHTS CREATION AND RECONSTRUCTION 25 (1998) ("The Sedition Act itself was a textbook example of attempted self-dealing . . . . [I]t criminalized libel of incumbents, but not of challengers.").

The Act's sunset clause was also seen as politically motivated. The law was set to expire the day before the new President would be inaugurated.[204] The timing was strategic: if Jefferson won the upcoming presidential election, then he could not use the statute to imprison his Federalist opponents.

Many Americans at the time saw these provisions as an attempt by the Federalist Party to suppress the emergence of an opposition party. The Kentucky and Virginia legislatures, in the ensuing months, passed resolutions condemning the Sedition Act as unconstitutional under the First Amendment.[205] These resolutions were, in fact, secretly written by Jefferson and Madison, but their passage is indicative of broader public support in certain states.

Hamilton, who had served as Secretary of the Treasury under the Washington and Adams administrations, condemned the Virginia and Kentucky Resolutions as a "conspiracy to overturn the government."[206] He advocated an aggressive response to the Resolutions, proposing that the government "attack and arraign its enemies" and that military forces "be drawn towards Virginia" to "put Virginia to the test of resistance."[207]

Ultimately, Adams demurred to the use of military force, and the Federalists lost the presidential election of 1800 as well as their majorities in the House and the Senate.[208] It marked the nation's first transfer of power

---

[204] Sedition Act of 1798, *supra* note 201 ("And be it further enacted, That this act shall continue and be in force until the third day of March, one thousand eight hundred and one, and no longer . . . ."); *see also* AMAR, *supra* note 203, at 25 ("Yet another dead giveaway: the act conveniently provided for its own expiration after the next election.").

[205] *See* Thomas Jefferson, The Kentucky Resolutions of 1798, *in* 30 THE PAPERS OF THOMAS JEFFERSON, *supra* note 114, at 529–43; James Madison, Virginia Resolutions (Dec. 21, 1798), *in* 17 THE PAPERS OF JAMES MADISON, *supra* note 202, at 185–91 (concluding that the Sedition Act represented a "palpable violation" of the rights that Americans had "declared and secured" in ratifying the First Amendment).

[206] Letter from Alexander Hamilton to Theodore Sedgwick (Feb. 2, 1799), *in* 22 THE PAPERS OF ALEXANDER HAMILTON 452–54 (Harold C. Syrett ed., 1975).

[207] *Id.* ("[T]he tendency of the doctrines advanced by Virginia and Kentucky to destroy the Constitution of the States—and, with calm dignity united with pathos, the full evidence which they afford of a regular conspiracy to overturn the government . . . . The Government must not merely defend itself but must attack."); *see also* BIRD, *supra* note 202, at 35 ("Secretary of State Timothy Pickering joined Hamilton in seeing the Virginia and Kentucky Resolutions as 'hostile to the General Government,' 'outrageous attempts to break the union,' and 'mad and rebellious resolves.' Other High Federalists, such as Sen. Theodore Sedgwick of Massachusetts, viewed the Virginia and Kentucky Resolutions as 'little short of a declaration of war.'").

[208] *See* BIRD, *supra* note 202, at 359 ("The Federalist sponsorship and enforcement of the Alien and Sedition Acts was a major factor in that party's demise, as those acts rallied and unified Republicans and contributed to the Republican Party's electoral victory in 1800 and

between political parties. Many see the Federalists' electoral loss as public backlash against the Sedition Act. The Federalists "would never again hold a majority in any legislative branch of the federal government, and, within a few short years, the party would cease to exist entirely."[209]

Although the Sedition Act's constitutionality was "never tested in" the Supreme Court, as none of those prosecuted under the Act had an opportunity to appeal, the Justices declared more than a century-and-a-half later that "the attack upon its validity has carried the day in the court of history."[210] Indeed, after winning the presidency in 1801, Jefferson pardoned all those who had been convicted under the Act and encouraged Congress to remit all fines imposed, declaring, "I discharged every person under punishment or prosecution under the sedition law, because I considered, and now consider, that law to be a nullity."[211]

Notably, throughout the entire episode—what many have called the first national controversy over "the central meaning of the First Amendment"[212]—neither party threatened, nor feared, regulation infringing on what at the time was pervasive usage of encrypted ciphers and codes by leaders of both political parties.

Records show that Jefferson and Madison depended on encrypted correspondence well before the Sedition Act crisis, as political tensions between the emerging Federalist and Republican factions mounted during the Washington administration.[213] As Secretary of State, Jefferson increasingly

---

its political dominance for a generation.").

[209] Tyler Broker, *Free Speech Originalism*, 81 ALB. L. REV. 45, 52 (2018); *see also* AMAR, *supra* note 203, at 25 ("[A] popular majority adjudicated the First Amendment question in the election of 1800, by throwing out the haughty and aristocratic rascals who had tried to shield themselves from popular criticism.").

[210] N.Y. Times Co. v. Sullivan, 376 U.S. 254, 276 (1964).

[211] Letter from Thomas Jefferson to Abigail Adams (July 22, 1804), *in* 44 THE PAPERS OF THOMAS JEFFERSON 129–31 (James P. McClure ed., 2019); *see also* Abrams v. United States, 250 U.S. 616, 629–30 (1919) (Holmes, J., dissenting) (noting Congress's later repayment of fines as evidence of the nation's "repentance for the Sedition Act of 1798").

[212] *Sullivan*, 376 U.S. at 273; *see also* William M. Carter, Jr., *The Second Founding and the First Amendment*, 99 TEX. L. REV. 1065, 1083–84 (2021) ("The Sedition Act of 1798 sparked the nation's first sustained controversy regarding the First Amendment's guarantee of freedom of speech."); LEONARD WILLIAMS LEVY, LEGACY OF SUPPRESSION: FREEDOM OF SPEECH AND PRESS IN EARLY AMERICAN HISTORY 258 (1960).

[213] *See, e.g.*, Letter from James Madison to James Monroe (Dec. 4, 1794), *in* 15 THE PAPERS OF JAMES MADISON 405–09 (Thomas A. Mason et al. eds., 1985) ("I should say more to you now, if I could say it in cypher."); Letter from Thomas Jefferson to James Madison (Aug. 11, 1793), *in* 25 THE PAPERS OF JAMES MADISON 54–56 (Thomas A. Mason et al. eds., 1985) ("[E]ncoded by Jefferson using the code he sent [James Madison] on 11 May 1785 . . . .").

found himself at odds with Hamilton over fundamental questions of federal power and foreign policy.[214] By 1793, Jefferson had resigned from Washington's cabinet,[215] and both he and Madison feared that their correspondence could be intercepted by Federalist-aligned postmasters. At times, in an apparent attempt to further distance themselves from their written communications on the off chance that their cipher was compromised, they also left their letters unsigned.[216]

On the other end of the political spectrum, Hamilton took up encryption during the Adams administration, both with political allies and family members, presumably in reaction to growing privacy concerns posed by the emergence of the nation's first opposition party.[217] Letters preserved among Hamilton's

---

[214] *See* LINDSAY M. CHERVINSKY, THE CABINET: GEORGE WASHINGTON AND THE CREATION OF AN AMERICAN INSTITUTION 12, 233 (2020) ("By 1793, Hamilton and Jefferson hated each other . . . . Their participation in the cabinet exacerbated partisan tensions and accelerated the development of the first party system.").

[215] Letter from Thomas Jefferson to George Washington (Dec. 31, 1793), in 27 THE PAPERS OF THOMAS JEFFERSON 585 (John Catanzariti ed., 1997) (formally resigning as Secretary of State). Jefferson had initially sought to resign in September 1793. Letter from Thomas Jefferson to George Washington (July 31, 1793), *in* 13 THE PAPERS OF GEORGE WASHINGTON, PRESIDENTIAL SERIES 311–12 (Christine Sternberg Patrick ed., 2007). On August 6, 1793, Washington expressed "regret at accepting a second term as president, and how much it was increased by seeing that he was to be deserted by those on whose aid he had counted," and successfully persuaded Jefferson to postpone his resignation until year's end. *Id.* at 312 n.3 (editorial note describing Jefferson's notes on his conversation with Washington on Aug. 6, 1793).

[216] *See, e.g.*, Letter from James Madison to Thomas Jefferson (May 22, 1796), *in* 29 THE PAPERS OF THOMAS JEFFERSON 108–10 (Barbara B. Oberg ed., 2002) (noting that letter is "unsigned" and encrypted in part); Letter from Thomas Jefferson to James Monroe (Sep. 6, 1795), *in* 28 THE PAPERS OF THOMAS JEFFERSON 448–51 (John Catanzariti ed., 2000) (observing that letter is "unsigned [and] written partly in code"); Letter from Thomas Jefferson to James Madison (Aug. 3, 1793), *in* 26 THE PAPERS OF THOMAS JEFFERSON 606–07 (John Catanzariti ed., 1995) (stating that letter is "unsigned" and "partly in code"). The practice of leaving letters unsigned or using pseudonymous signatures to hide the author's identity was not limited to political communications. Abigail Adams, for instance, signed letters to her husband John Adams with the pseudonym "Portia"—a reference to the wife of Brutus, known for her wisdom and strength. *See, e.g.*, Letter from Abigail Adams to John Adams (July 21, 1776), *in* 2 THE ADAMS PAPERS, ADAMS FAMILY CORRESPONDENCE 55–57 (L. H. Butterfield ed., 1963) (endorsing letter as pseudonym "Portia" and writing "I have no doubt but that my dearest Friend is anxious to know how his Portia does"); *see also* Letter from John Adams to Abigail Adams (Nov. 24, 1792), *in* 9 THE ADAMS PAPERS, ADAMS FAMILY CORRESPONDENCE 330–31 (C. James Taylor et al. eds., 2009) (addressing letter to pseudonym "Portia" and alternately "My dearest Friend"); Letter from John Adams to Abigail Adams (May 12, 1780), *in* 3 THE ADAMS PAPERS, ADAMS FAMILY CORRESPONDENCE 338–39 (L. H. Butterfield & Marc Friedlaender eds., 1973) (addressing letter to pseudonym "My dear Portia").

[217] *See, e.g.*, Letter from Philip Schuyler to Alexander Hamilton (June 6, 1799), *in* 23 THE PAPERS OF ALEXANDER HAMILTON 173 (Harold C. Syrett ed., 1976) ("I shall transmit you the Cypher by Capt: Bogert."); Letter from Alexander Hamilton to Gouverneur Morris (June 22, 1792), *in* 11 THE PAPERS OF ALEXANDER HAMILTON 545–46 (Harold C. Syrett ed., 1966) ("Will it not be a

papers indicate a hesitancy to write candidly absent use of a previously agreed-upon cipher. Months before the election of 1800, for example, Hamilton wrote Founder and Federalist ally Rufus King, "If the projected cypher was established I should now have very much to say to you," indicating that even amid one of the most troubling First Amendment crises the nation has seen, those of all political persuasions relied on encryption to safeguard their written communications.[218]

The fact that the Federalists were willing to imprison critics for mere political speech but drew the line at regulating encryption is telling. That line, drawn even in the heat of partisan fervor, reveals what the Founding generations believed lay beyond government reach.

IV. CONCLUSION

Although no Justice "seems to question that history has a role to play" in defining the contours of First Amendment coverage, some have openly questioned the burden that historical inquiry places on already cluttered court dockets.[219] As Justice Jackson laments, "just canvassing the universe of historical records and gauging the sufficiency of such evidence is an exceedingly difficult task."[220] As she explains, recent cases "highlight[] [the] apparent difficulty faced by judges on the ground."[221]

This Article answers the call for historical scholarship on a pressing and unresolved First Amendment question. Without any precedent on point to guide the Court, the Justices have little choice but to begin from First Amendment first principles.[222] This Article has accordingly scoured archival

---

necessary preliminary to agree upon a Cypher? One has been devised for me, which though simple in execution is tedious in preparation. I may shortly forward it.").

[218] Letter from Alexander Hamilton to Rufus King (Jan. 5, 1800), *in* 24 THE PAPERS OF ALEXANDER HAMILTON 167–71 (Harold C. Syrett ed., 1976).

[219] *See, e.g.*, United States v. Rahimi, 602 U.S. 680, 1905 (Sotomayor, J., concurring); *id.* at 740–43 (2024) (Jackson, J., concurring); *see also* Campbell, *supra* note 44, at 313 ("Most judges and scholars incorporate history into their interpretative method in some way.").

[220] *Rahimi*, 602 U.S. at 745 (Jackson, J., concurring).

[221] *Id.* at 741–42 ("In my view, as this Court thinks of, and speaks about, history's relevance to the interpretation of constitutional provisions, we should be mindful that our common-law tradition of promoting clarity and consistency in the application of our precedent also has a lengthy pedigree. So when [lower] courts signal they are having trouble with one of our [historical] standards, we should pay attention.").

[222] *Cf.* Wesley J. Campbell, *Commandeering and Constitutional Change*, 122 YALE L.J. 1104, 1180 (2013) ("History may help guide our thinking on these constitutional issues, but it does not resolve how we should account for changing circumstances or how the Court should

records in search of evidence that may be illuminative of practice in the years leading up to ratification and shortly thereafter. It has found not only that encryption flourished without government restriction during the Founding era, but also that it has played an essential role in events foundational to the development of the nation, including the drafting of the First Amendment itself. In tracing the private correspondence of America's foremost leaders at the Founding, as well as doctors, lawyers, and businessmen of the era, it has uncovered a forgotten, yet deeply cherished, tradition of association and advocacy.

Letters preserved in the private libraries of the Founders, including that of the nation's first Chief Justice, show that many remained insistent on encrypting their personal and professional letters, despite the considerable effort required, due to the fraught nature of postal transit in early America. In a time before envelopes, in which wax seals could be easily broken, encryption remained the only reliable guarantee of a letter's security against interception en route or untrustworthy couriers.

The Founders' uses of encryption spanned business matters, political matters, familial matters, and even matters of the heart. Although Adams and Jefferson would ultimately emerge as the nation's leading political rivals, one area of common ground is their agreement that courtship letters ought to be encrypted.

Historical records demonstrate that Jefferson's instigation and revision of the Bill of Rights (from three thousand miles away in Paris) may not have been possible absent an encrypted cipher with fellow Virginian and lifelong friend Madison, who introduced the draft to Congress in 1789.[223] In the years following ratification, the pair's reliance on encrypted correspondence grew, so much so that Jefferson and Madison began leaving their letters unsigned, in an apparent attempt to further distance themselves from their written communications in the off chance that their cipher was compromised.

The Sedition Act of 1798, which criminalized criticism of the President, is a revealing test case for Founding-era views on encrypted speech. The Federalist Party wielded federal power to imprison political opponents for their words, yet neither those in power nor the opposition contemplated restricting the

---

incorporate prudential considerations into its constitutional analysis.").

[223] 1 Annals of Cong. 440, 444 (1789) (Joseph Gales ed., 1834) (statement of Rep. James Madison) (proposing the amendments as a means to "stifle[] the voice of complaint" and secure the loyalty of citizens who otherwise "doubted the merits of the Constitution").

widespread use of encryption. Indeed, Hamilton—a leading architect of the Sedition Act's enforcement—himself took up encryption in his correspondence with political allies and family members, apparently viewing it as an essential tool for privacy as political tensions mounted. It is telling that even during the nation's darkest moment for free speech, when those in power criminalized political dissent itself, encryption remained sacrosanct—unregulated, unquestioned, and wielded by the Act's own architects.

Skeptics of constitutional privacy rights often observe that the word "privacy" appears nowhere in the Bill of Rights. They caution that courts must resist the temptation to read contemporary values into constitutional text. But encryption, it turns out, is not a contemporary practice seeking refuge in old text. It is an eighteenth-century practice reborn in digital form.

Today's debates over encrypted messaging are not new—they are old anxieties in modern dress. Americans once worried about postmasters opening their letters; now they worry about the government monitoring their texts. The medium has changed—parchment has given way to pixels—but the underlying concern remains constant: the need to communicate privately, free from surveillance by those in power.