Autonomy Through Anonymity: Reconceptualizing Privacy Enhancing Tools Under the U.S. Constitution

By Aaron Daniel

Bernstein v. Department of State - A Roadmap for Defending Free Speech and Privacy

"Code is speech."[1] In 1996, these three groundbreaking words set the precedent that source code, like any other language, is entitled to protection under the First Amendment to the United States Constitution. Professor Daniel Bernstein challenged the United States Department of State, which barred him from publishing and sharing his encryption algorithms abroad, and won. The government could not, within its boundless discretion, impose prior restraints on his ability to publish source code.

The Bernstein decision's iconic ruling is well-known among cypherpunks, legal scholars, and free speech advocates. Rarely discussed is a secondary argument Bernstein advanced related to the unique function of his source code. Bernstein made the bold claim that not only was his encryption code speech, but it was especially protected speech because it enabled modes of communication the constitution prioritizes as essential to liberty; ***private***, ***anonymous*** speech.

Bernstein's pleadings cited Supreme Court precedent that held the "**First Amendment includes the right to speak confidentially**".[2] it "**protects anonymous speech".**[3] and it **"prevents compelled disclosure** of those with whom one associates and speaks".[4] In short, Bernstein argued the First Amendment preserves "the ***autonomy*** to control one's own speech".[5] Cryptography enabled private and anonymous digital communications, and thus Bernstein concluded it was "inherently imbued with First Amendment significance".[6]

The court in Bernstein did not rule on his argument that encryption was entitled to First Amendment protections ***because*** it "facilitates private communication".[7] The court reasoned it was not necessary to imbue cryptography specifically with protections, since it was ruling that all

---

[1] Bernstein v. U.S. Dep't of State, 922 F. Supp. 1426, 1436 (N.D. Cal. April 15, 1996).
[2] Plaintiff's Opposition to Motion to Dismiss, Bernstein, 922 F. Supp. 1426 (No. 95-0582).
[3] Id.
[4] Id.
[5] Id.
[6] Plaintiff's Memorandum of Points and Authorities in Support of Motion for Partial Summary Judgment, Bernstein v. U.S. Dept' of State, 945 F. Supp. 1279 (N.D. Cal. Dec. 6, 1996) (95-0582).
[7] Bernstein, 945 F. Supp. 1279, 1287.

code was protected. The theory that privacy and anonymity enhancing tools could be entitled to special protections under the constitution was thus resigned to the dust-bin of legal history and forgotten.

Until now.

The right to anonymity advanced by Bernstein finds support in the history of America's founding. And recent U.S.Supreme Court precedent indicates renewed support for said right. The legal system isn't the only avenue through which to secure individual rights to privacy and anonymity, nor even the most effective, but favorable rulings can shield efforts to build the privacy and anonymity solutions necessary to advance society. Recent events like asset freezes against Canadian protesters, sanctions against the entity and code behind Tornado Cash, and even incarcerations for peer-to-peer bitcoin transactions, have underscored that individuals need privacy enhancing tools. Privacy guards against what one legal scholar has described as "a particular kind of creeping totalitarianism, an unarmed occupation of individuals' lives".[8]

The right to anonymity, then, is not just important in and of itself; it is necessary to the preservation and realization of individual autonomy.

Anonymity Is Essential for Individual Autonomy

> The word "**autonomy**" is derived from the Greek stems for "self" and "law" and means literally "the having or making of one's own laws". Its sense therefore can be rendered at least approximately by such terms as "self-rule", self-determination", "self government", and "independence".[9]

In other words, autonomy can be considered "the **sovereign** authority to govern oneself, which is absolute within one's own moral 'boundaries'".[10] Privacy and its more complete cousin, anonymity, can create those sovereign boundaries.

The erosion of privacy is so much more than a psychic harm (the "creepiness" of being spied on). It strikes at our basic human right to self determination. "Privacy" is not just, as Justice Brandeis first posited, "the right to be left alone". That definition removes all agency from the individual and leaves them at the mercy of the state, and other members of society, be they corporate or natural, to refrain from surveilling our lives. But the last two decades have shown neither the state nor big tech are inclined towards restraint.

Eric Hughes' definition of "privacy" in his 1993 Cypherpunk's Manifesto restores individual agency: it is "**the power to selectively reveal oneself** to the world". Justice Murphy similarly explained the importance of privacy in a 1942 dissent rejecting the warrantless use of

---

[8] Jed Rubenfeld, The Right of Privacy, 102 Harv. L. Rev. 737, 785 (1989).
[9] Joel Feinberg, Autonomy, Sovereignty, and Privacy: Moral Ideals in the Constitution?, 58 Notre Dame L. Rev. 445, 447 (1983)
[10] Id.

eavesdropping technology, opining "the spiritual **freedom** of the individual depends in no small measure upon the preservation of that right", and that "[i]nsistence on its retention does not mean that a person has anything to conceal, but means rather that **the choice should be his as to what he wishes to reveal".**[11]

Two decades later, Justice Douglas dissented in a case approving use of an informant wearing a "wire", recognizing that when privacy is lost, so too is freedom:

> "If a man's privacy can be invaded at will, who can say he is free? If his every word is taken down and evaluated, or if he is afraid every word may be, who can say he enjoys **freedom of speech**? If his every association is known and recorded, if the conversations with his associates are purloined, who can say he enjoys **freedom of association**? When such conditions obtain, our citizens will be afraid to utter any but the safest and most orthodox thoughts; afraid to associate with any but the most acceptable people. **Freedom as the Constitution envisages it will have vanished.**"[12]

Privacy and anonymity grant individuals the freedom to exercise all other rights guaranteed by the constitution. Thus, a tyrant most efficiently undermines liberty by curtailing privacy. Justice Robert Jackson, who took a leave from the Court to prosecute Nazi war criminals at the Nuremberg trials, acknowledged this within the context of the Fourth Amendment:

> "Among deprivations of rights, none is so effective in cowing a population, crushing the spirit of the individual and putting terror in every heart. Uncontrolled search and seizure is one of the first and most effective weapons in the arsenal of every arbitrary government. And one need only briefly to have dwelt and worked among a people possessed of many admirable qualities but deprived of these rights to know that the human personality deteriorates and dignity and self-reliance disappear where homes, persons and possessions are subject at any hour to unheralded search and seizure by the police."[13]

Privacy and anonymity, then, are foundational to preserving individual autonomy. They are the bedrock upon which all other human rights are established.

Historical Origins of the Rights to Privacy and Anonymity in America

Ample historical evidence demonstrates that privacy safeguards the exercise of other fundamental rights. The right to anonymity, and particularly anonymous speech, is not a newly

---

[11] Goldman v. U.S., 316 U.S. 129, 137 (1942) (Murphy, J., dissenting).
[12] Osborn v. U.S., 385 U.S. 323, 353-54 (1966) (Douglas, J., dissenting).
[13] Brinegar v. United States, 338 U.S. 160, 180-81 (1949) (Jackson, J., dissenting).

discovered right. The right was rooted in the earliest American experiences and then bloomed at the nation's Founding.

When the Pilgrims landed on Plymouth Rock, they were fleeing an insidious type of religious persecution where surveillance was weaponized against minorities. Queen Elizabeth "built a network of spies and informants to root out perceived threats to her reign", which included Catholics and Puritan Separatists, who we know as the "Pilgrims".[14] The population was turned against one another, minorities "feared that their neighbors would report them", and Elizabeth's successor, James I, "created a series of bounties to reward people for turning in" religious minorities.[15] A famous portrait of Queen Elizabeth portrays her in a gown "embroidered in human eyes and ears".[16] That was the dystopia some of the first American colonists fled. Until the Pilgrims landed in North America, religious liberty was only achievable through privacy.

A century later, two well-known English court cases would inspire the Founders to pass the Fourth Amendment, which protects individuals' "persons, houses, papers, and effects, against unreasonable searches and seizures". But the root of each case was the right to free speech, now protected by the First Amendment. In Entick v. Carrington and Wilkes v. Wood, political pamphleteers critical of the King and his ministers had their homes ransacked and their papers and effects seized in furtherance of seditious libel charges.[17] Both Entick and Wilkes sued the officials responsible for the raid and won damages based on violations of their rights to privacy and anonymity.

Upholding the jury verdict for Entick, the judge ruled "where **private** papers are removed and carried away, the **secret nature** of those goods will be an aggravation of the trespass, and demand more considerable damages in that respect".[18] Although the seizures were authorized by warrant, that did not permit the King's men to violate Entick's right of privacy.

The decision in Wilkes's case can be seen as upholding the even broader right to anonymity against censorship. John Wilkes was a well-known Member of Parliament who anonymously authored a series of pamphlets criticizing the King.[19] As the pamphlet's author was anonymous, a general warrant was issued naming no one specifically, but instead directed the King's officials "to make strict and diligent search for the authors, printers and publishers" of the allegedly seditious pamphlet, and to seize them and their papers.[20] Forty-nine suspects, including Wilkes, were arrested and their private papers seized. The judge instructed the jury on the danger of general warrants, stating "if such a power is truly invested in a secretary of state, and he can delegate this power, it certainly may affect the person and property of every man in this

---

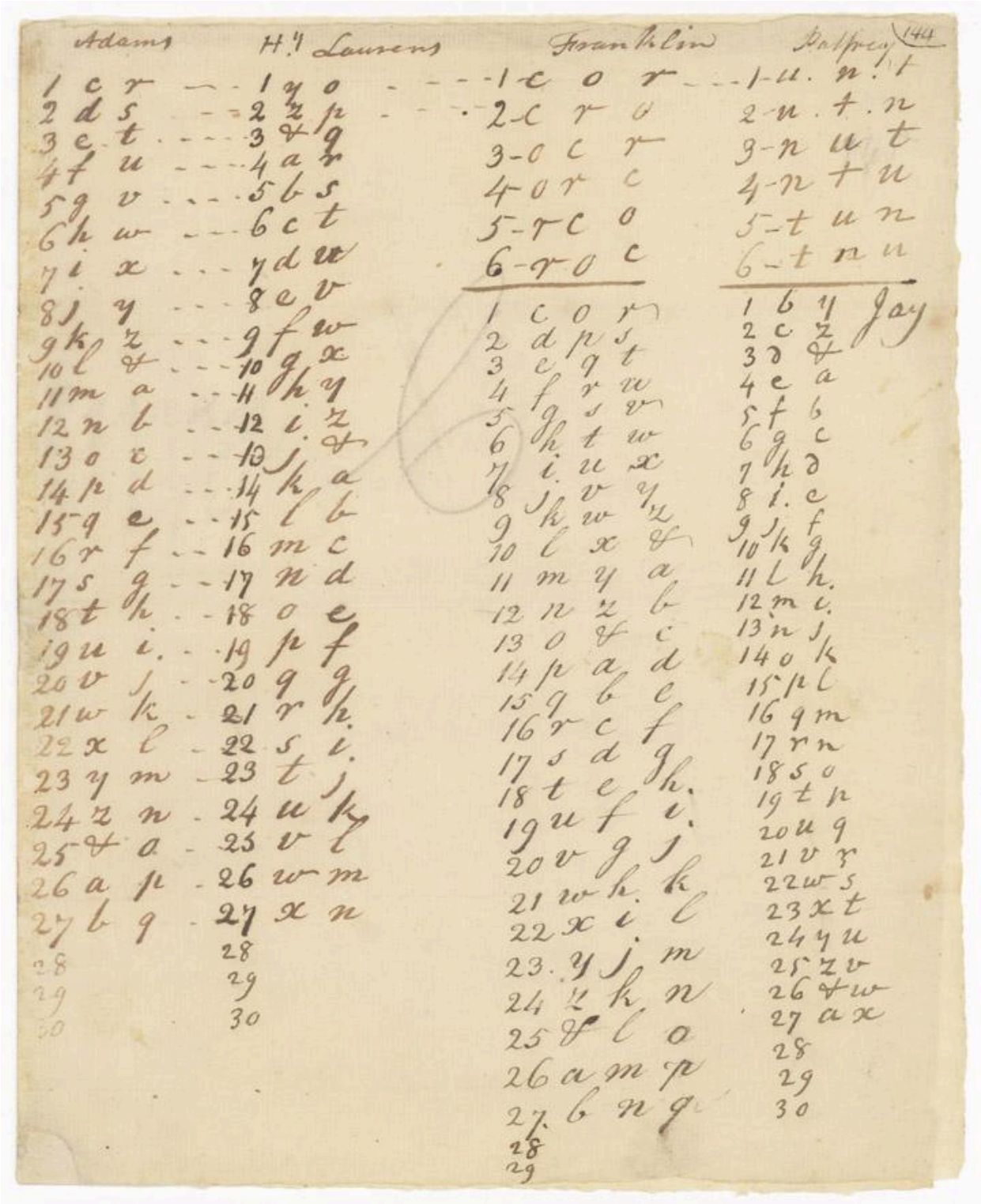
[14] Alvaro M. Bedoya, Privacy as a Civil Right, 50 N.M. L. Rev. 301, 307-08 (2020).
[15] Id.
[16] Id.
[17] William Stuntz, The Substantive Origins of Criminal Procedure, 105 Yale L.J. 393, 396-98 (1995).
[18] Id.
[19] Id.
[20] Id.

kingdom, and is **totally subversive of the liberty of the subject**".[21] The jury awarded Wilkes one thousand pounds in damages.

By the time of the Revolution, Americans were not just espousing the right to privacy as an ideal, they were actively practicing it. Founding-era use of privacy enhancing tools was common. One of the most widely used encryption systems amongst the Founders was the Lovell Cipher, created by James Lovell, a member of congress who served on the Committee for Foreign Affairs.

Lovell's cipher involved writing two vertical columns of the alphabet next to a third vertical column of the numbers 1-27. If the correspondents knew the keyword (for example, John Adams's was "CR") they knew which letters of the alphabet to start each column with (ampersand was included). The enciphering party would then substitute each letter with the corresponding number, alternating rows for each letter.

[21] Id.



[image of lovell ciphers used by peace commission: https://catalog.archives.gov/id/2450021]

The Lovell Cipher was used extensively by U.S. diplomats during and after the war (including by the peace commission in France), the army, and individual Founders for personal matters. For example, Abigail Adams was initially reluctant to use the inconvenient cipher, but later relented

after learning that her letters with husband John were being intercepted, forcing John to be more guarded in his correspondence. In a June 17, 1782 letter, Abigail provided John tips on how to use the Lovell Cipher to decipher encrypted messages.[22]

Thomas Jefferson was an advanced cryptographer, even designing his own wheel cipher, a version of which was in use by the U.S. Army well into the 20th century. One of the most compelling pieces of evidence suggesting the Founders considered private speech a fundamental right is an August 28, 1789 letter from Jefferson to James Madison. In it, Jefferson encoded sensitive information about French revolutionaries in ciphertext, and just a few lines later proposed edits to Madison's draft of the First Amendment.[23]

[images of august 28 letter with ciphertext https://www.loc.gov/resource/mjm.04_0183_0189/?st=gallery]

And although Aaron Burr used enciphered correspondences in his plot to establish a new government in the West, the mere use of such privacy enhancing techniques was not deemed evidence of criminality at his trial.[24] Using privacy tools to communicate was perfectly normal for the time.

It is, therefore, entirely accurate to say that the United States was founded, in part, through private and anonymous speech. The Founders would have considered the existence of such a right noncontroversial.

Recent Precedent Indicates Renewed Support for Privacy and Anonymity

In a concurrence upholding the right to anonymous political speech, Justice Clarence Thomas observed that the “Framers’ universal practice of publishing anonymous articles and pamphlets, indicates that the Framers shared the belief that such activity was firmly part of the freedom of the press”.[25] And, he continued, it “is only an innovation of modern times that has permitted the regulation of anonymous speech”.

---

[22] Letter from Abigail Adams to John Adams, 17 June 1782, with a List of Articles Wanted from Holland [electronic edition], Adams Family Papers: An Electronic Archive, Massachusetts Historical Society, http://www.masshist.org/digitaladams/.

[23] John 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, 43 (1997).

[24] Fraser, at 57.

[25] McIntyre v. Ohio Elections Comm’n, 514 U.S. 334, 367 (1995) (Thomas, J., concurring).

Justice Thomas was using the term “innovation” sardonically. It’s a bitter irony that the most persuasive defenses of the right to privacy and anonymity have been offered in dissent. The rise of the modern-day surveillance state can be plotted out by 20th century Supreme Court decisions authorizing ever more intrusive means of data collection and deanonymization, ostensibly for the purpose of fighting crime.

But two recent decisions indicate a renewed interest in protecting these rights. The current Court may be open to considering Bernstein’s argument that privacy-enhancing code is particularly important speech under the First Amendment.

The first decision is Carpenter v. U.S., where the Court held that warrantless acquisition of cell-site location information (CLSI) violated the Fourth Amendment as an unreasonable search. The Court declined to apply the Third-Party Doctrine, which holds that an individual loses the expectation of privacy by disclosing information such as financial data to a third-party in the course of regular business, to CSLI. The Court held a “person does not surrender all Fourth Amendment protection by venturing into the public sphere”.[26]

Interestingly, although four justices dissented, at least two did so because they wished to extinguish the Third-Party Doctrine and the “reasonable expectation of privacy test” altogether. Justices Thomas and Gorsuch suggested that the Court return to a **property based** understanding of privacy that better reflects the intention of the Founders. Under this approach, Justice Gorusch suggested, “[j]ust because you entrust your **data**—in some cases, your **modern-day papers and effects**—to a third party may not mean you lose any Fourth Amendment interest in its contents”.[27] Now imagine your data is cryptographically shielded from third-party inspection, much like a sealed envelope placed into the mail, which the Supreme Court has long protected from warrantless searches.

The second decision indicating renewed emphasis on individual privacy is Americans for Prosperity Foundation v. Bonta, issued just last year. In Bonta, the Court reaffirmed the right to anonymous speech in the context of monetary donations. The Court struck down a California regulatory scheme that required charities to report the names and addresses of all donors who gave over $5,000. The Court’s majority emphasized “the vital relationship between freedom to associate and **privacy in one’s associations**.”[28] Bonta thus has important implications for Bitcoin, and financial privacy in general, as it can be read as protecting an individual right to anonymous spending.

---

[26] Carpenter v. U.S., 138 S. Ct. 2206, 2217 (2018).
[27] Id. at 2269.
[28] Ams. for Prosperity Found. v. Bonta, 141 S.Ct. 2373, 2382 (2021)

Bitcoin Empowers Individuals to Practice Privacy and Achieve Autonomy

When the Bill of Rights was adopted, communications were far more secure than they are today. Financial transactions were easier to keep private, too.

But modern technology and the gradual accretion of resources and personnel to the state has broadened Federal power into something more closely resembling that wielded by the British Empire than the United States, as the Founders originally envisioned it.

The Founders collectively severed their relationship with a government that had unfettered power over their lives. When they reconstituted their relationship to government, they constrained its power with a constitution that granted it limited permissions.

Today, to regain autonomy, individuals must sever their relationships with a government that has gained too much power over their lives. By erecting a bulwark of privacy, individuals can again constrain government with limited permissions, choosing for themselves when and where to let the state into their lives.

The legal system has a checkered history of protecting individual liberties. Indeed, activity that was legal yesterday may not be tomorrow. Two generations of American women possessed the right to autonomy over their bodies until "settled precedent" changed. What other rights established under the rule of law may be lost tomorrow? The right to marital privacy (Griswold v. Connecticut)? The right to make family planning decisions (Eisenstadt v. Baird)? The right to make consensual love with whomever one choses (Lawrence v. Texas)?

Only by remaining anonymous and cultivating informational privacy can the individual truly ensure personal autonomy. Anonymity and privacy protect the individual against both the tyranny of the majority and the vicissitudes of the common law court system.

Fortunately, while the rest of society ignored the slow erosion of their civil liberties, the cypherpunks never stopped "writ[ing] code".[29] Satoshi Nakamoto mixed that code into a unique combination that was greater than the sum of its parts, creating Bitcoin. Bitcoin provides the decentralized foundation on which new and powerful privacy enhancing tools are being deployed to empower individuals to control their information and defend their autonomy.

For example, coinjoin transactions facilitated by software such as whirlpool or joinmarket obfuscate transaction histories on the otherwise transparent Bitcoin blockchain without the user giving up custody of their bitcoin. The lighting network, a faster, second protocol layer rooted to the Bitcoin protocol's immutable settlement process, uses a networking solution called "onion

[29] Eric Hughes, A Cypherpunk's Manifesto (1993), https://nakamotoinstitute.org/static/docs/cypherpunk-manifesto.txt.

routing" to ensure private payment routing. And a newer protocol called Fedimint uses blinded cryptographic signatures in a community custodial model to achieve financial privacy.

Because all of these open source software projects enable private and anonymous digital communications of value, Bernstein's argument that they are "inherently imbued with First Amendment significance" should apply. Thus, while the legal system may not be the ideal solution to privacy at scale, it can provide protections to code that enables privacy and anonymity. If code is protected speech, and private or anonymous speech is also protected, then privacy-enabling code is entitled to the highest constitutional protections. Like the Founders who designed and used new cryptographic systems in the pursuit of liberty, it's time for individuals to code and use privacy enhancing tools to regain autonomy.

.