The Cultural Contradictions of Cryptography:
A History of Secret Codes in Modern America

Charles Berret

Submitted in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy
under the Executive Committee
of the Graduate School of Arts and Sciences

Columbia University
2019

Abstract

The Cultural Contradictions of Cryptography

Charles Berret

This dissertation examines the origins of political and scientific commitments that currently frame cryptography, the study of secret codes, arguing that these commitments took shape over the course of the twentieth century. Looking back to the nineteenth century, cryptography was rarely practiced systematically, let alone scientifically, nor was it the contentious political subject it has become in the digital age. Beginning with the rise of computational cryptography in the first half of the twentieth century, this history identifies a quarter-century gap beginning in the late 1940s, when cryptography research was classified and tightly controlled in the US. Observing the reemergence of open research in cryptography in the early 1970s, a course of events that was directly opposed by many members of the US intelligence community, a wave of political scandals unrelated to cryptography during the Nixon years also made the secrecy surrounding cryptography appear untenable, weakening the official capacity to enforce this classification. Today, the subject of cryptography remains highly political and adversarial, with many proponents gripped by the conviction that widespread access to strong cryptography is necessary for a free society in the digital age, while opponents contend that strong cryptography in fact presents a danger to society and the rule of law. I argue that cryptography would not have become

invested with these deep political commitments if it had not been suppressed in research and the media during the postwar years. The greater the force exerted to dissuade writers and scientists from studying cryptography, the more the subject became wrapped in an aura of civil disobedience and public need. These positive political investments in cryptography have since become widely accepted among many civil libertarians, transparency activists, journalists, and computer scientists who treat cryptography as an essential instrument for maintaining a free and open society in the digital age. Likewise, even as opponents of widespread access to strong cryptography have conceded considerable ground in recent decades, their opposition is grounded in many of the same principles that defined their stance during cryptography's public reemergence in the 1970s. Studying this critical historical moment reveals not only the origins of cryptography's current politics, but also the political origins of modern cryptography.

Table of Contents

Introduction

The Cultural Contradictions of Cryptography

In early 2012, when the NSA whistleblower Edward Snowden was still forming plans for his disclosures to the press, he corresponded with documentarian Laura Poitras over encrypted email, concealing their conversation from the electronic surveillance programs that Snowden himself would soon reveal to the public in a leak of classified documents. In these early exchanges with Poitras, Snowden chose to remain anonymous. He went by the pseudonym "Citizenfour,"[1] gesturing to three NSA whistleblowers who had tried and failed to blow the whistle before him.[2] In communications (and attempted communications) with other journalists, Snowden chose pseudonyms that were equally laden with political consideration, such as Cincinnatus and Publius, the former an icon of virtuous citizenship during the Roman republic, the latter a pseudonym used by several founding fathers of the United States

[1] Poitras, in turn, used this pseudonym as the title for her documentary which chronicled the Snowden leaks, *Citizenfour* (2014).

[2] The NSA whistleblowers who preceded Snowden in attempting to reveal the Agency's mass surveillance program were Thomas Drake, William Binney and J. Kirk Wiebe. NB: an earlier whistleblower, James Bamford, had been successful in his public disclosure of NSA operations in his book *The Puzzle Palace* (1982).

in a series of philosophical essays known as the Federalist Papers.[3] Poitras and Snowden would continue corresponding for several months, brokering connections with journalists at the Guardian and Washington Post who slowly came to share Poitras's confidence that their still-anonymous source really would deliver the historic leak he promised.[4] Over these tense months, during Snowden's private conversation with Poitras, he often reflected on the complex political dimensions of the events to come. He considered the possible outcomes of his disclosures, pondered the conditions necessary for genuine change, and assessed the forces working with and against their cause.

> The shock [among the public at seeing these documents] will provide the support needed to build a more equal internet, but this will not work to the advantage of the average person unless science outpaces law. By understanding the mechanisms through which our privacy is violated, we can win here. We can guarantee for all people equal protection against unreasonable search through universal laws, but only if the technical community is willing to face the threat and commit to implementing over-engineered solutions. In the end, we must enforce a principle whereby the only way the powerful may enjoy privacy is when it is the same kind shared by the ordinary: one enforced by the laws of nature, rather than the policies of man.[5]

It is worth reading this passage closely, for Snowden offers a theory of the relationship between science, law, and power that hinges on digital cryptography — communication software that conceals the contents of a message using complicated math. Today's cryptography rests on algorithms that, by the apparent laws of nature, are difficult or

[3] The 85 essays making up the Federalist Papers were written by Alexander Hamilton, James Madison, and John Jay and published in newspapers like the *Independent Journal*, the *New York Packet*, and *The Daily Advertiser* between 1787-8.

[4] Snowden chose not to contact journalists at the *New York Times* because they had mismanaged three previous attempts to blow the whistle on NSA's domestic spying program.

[5] Quoted in Glenn Greenwald, *Nowhere to Hide*, (Henry Holt and Co), p. 13.

even impossible to reverse without possessing the corresponding key. Snowden posits that the public can place its faith in encryption technology since it secures communications by way of proven mathematics and sound engineering, whereas the legal right to privacy had ceased to be enforced, and thus rendered moot the assumption that our rights could be protected through legislation alone. Unlike Alexander Hamilton, John Jay, and James Madison, the founding fathers who adopted the name "Publius" (also meaning "citizen") to argue for the passage of a Constitution to protect a set of fundamental liberties, Snowden backs away from faith in the "laws of man" and places it instead in the laws of nature and a technical community committed to "over-engineered" solutions to protect the right to privacy. Upon delivering the first round of leaks to a carefully chosen cadre of journalists, Snowden included a cover letter underlining this political stance:

> While I pray that public awareness and debate will lead to reform, bear in mind that the policies of men change in time, and even the Constitution is subverted when the appetites of power demand it. In words from history: *Let us speak no more of faith in man, but bind him down from mischief by the chains of cryptography*.[6] (emphasis added)

Here, Snowden subverts a familiar quote from Thomas Jefferson on tyranny and the rule of law: "…in questions of power then, let no more be heard of confidence in man, but bind him down from mischief by the chains of the constitution."[7] (again, emphasis added) In short, Snowden treats cryptography as a means to safeguard liberty and contain the evils of government in our time — not the legal authority of a document,

[6] Greenwald, *No Place to Hide*, p. 24.

[7] Thomas Jefferson, "Fair Copy of the Kentucky Resolutions of 1798."

even a Constitution that is often treated as essentially sacred,[8] but rather the mathematical authority of encryption, which they treat as an instrument of an even higher order.

Like Snowden, the WikiLeaks founder and radical transparency activist Julian Assange has endorsed a Promethean view of cryptography, but an even stronger one, treating the means of concealing information as a force inherently in favor of empowering the powerless in political resistance. Assange once referred to cryptography as "the ultimate form of non-violent direct action," adding that "no amount of coercive force will ever solve a math problem."[9] Assange traces his own ethos to a group known as the crypto-anarchists, or cypherpunks, who gathered in the early nineties around a shared interest in discussing and promoting all manner of radical social change that could be facilitated by modern cryptography. They discarded conventional ethics, treating such dicta as constrictive, and endeavored to map the range of new affordances that would follow from the development of modern cryptography.[10] Reflecting on these early days of crypto-anarchy from the pulpit he had built in 2012, Assange described the crypto-anarchists' initial, thrilling coalescence around the idea that mathematics, marshaled in software, could be a tool for transformative change against once-forbidding odds.

---

[8] See Michael Warner's *Letters of the Republic*, which tracks the emergence of the textual authority now invested in the U.S. Constitution and Bill of Rights.

[9] Julian Assange, et al., *Cypherpunks: Freedom and the Future of the Internet*, p. 5.

[10] The most controversial and divisive topic of conversation among the cypherpunks was a discussion of how to build a fully anonymous market to order assassinations and pay the killers while hiding the transaction with encryption.

> We discovered something. Our one hope against total domination. A hope that with courage, insight and solidarity we could use to resist. A strange property of the physical universe that we live in. *The universe believes in encryption. It is easier to encrypt information than it is to decrypt it.* We saw we could use this strange property to create the laws of a new world. To abstract away our new platonic realm from its base underpinnings of satellites, undersea cables and their controllers. To fortify our space behind a cryptographic veil. To create new lands barred to those who control physical reality, because to follow us into them would require infinite resources. And in this manner to declare independence.[11] (emphasis added)

Here, Assange depicts the political and social hopes that he and his cohort have invested in encryption — a set of uses that appears to rest upon the very structure of the natural world as represented through mathematics. This vision is packaged with rhetoric that rings the first-wave cyberculture's commitment to a fantastic vision of cyberspace, a frontier seemingly unencumbered by the fetters of the material world and its entrenched systems of power.[12]

In Assange's case, these appeals to the political affordances of cryptography evince full-on metaphysical commitments, whereas Snowden's outlook of cryptography's political potential rests on the committed, purpose-driven work of computer programmers and engineers instead. It is one thing to say, as Snowden does, that artifacts have inherent politics which reflect the intentions behind their design.[13] To say that physics or mathematics could have inherent political tendencies is, on the other hand, a claim from another plane entirely. And yet, this is Assange's plucky

---

[11] Julian Assange, et al., *Cypherpunks: Freedom and the Future of the Internet*, p. 4.

[12] For the definitive statement of cyberspace as a liberated digital utopia, see John Perry Barlow, "Declaration of the Rights of Cyberspace," in Ludlow, Peter. *High Noon on the Electronic Frontier : Conceptual Issues in Cyberspace*. Cambridge, Mass: MIT Press, 1996.

[13] For the classic statement of this position, see Winner, Langdon. "Do Artifacts Have Politics?" *Daedalus* 109, no. 1 (1980): 121–36.

argument: when a cryptographic algorithm scrambles a message, rendering it indistinguishable from the noise on a dead radio channel, the difficulty of reconstructing the original message should be treated as a structural feature of our universe that favors hiding information over revealing it. Even if that were true, it is unclear why this should present an inherent advantage to the powerless over the powerful, even if this advantage does require "courage, insight and solidarity." Snowden's claim is more subtle. He lays the burden on software developers to design secure communication tools that harness mathematics and statistical principles in a deliberate effort to protect the privacy of digital communications. An ardent libertarian, Snowden had hoped for his disclosure of government surveillance programs to underline the need for the general public to bolster these long-established rights using technology in light of the realization that the government could not be trusted to do so, even for rights enshrined in law. The most salient point of agreement between Snowden and Assange in these passages is the belief that cryptography could be more powerful than the law itself, or at least more reliable in carrying out the purpose stated in the letter of the law, since cryptographic security is grounded in rigid principles of math and physics rather than something as sloppy and unreliable as the coordination of social action. This echoes the legal scholar Lawrence Lessig's popular digital maxim 'code is law.'[14] That is to say, real power may flow from computer code, just as real power may flow from the letter of the law.

[14] Lessig, Lawrence. *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999. See also Alexander R. Galloway, *Protocol: How Control Exists after Decentralization*. Cambridge, Mass: MIT Press, 2004.

This particular image of cryptography may take on characteristics of the sublime. For a message to be rendered utterly impenetrable, its contents totally unreadable, could make it appear boundless, even beautiful in its inscrutability. An unreadable wall of digital text may inspire awe, wonder, even a hint of uneasiness. Like hieroglyphs, which once provided a deep reserve of fantasy precisely because they could potentially mean anything at all, decipherment is tantamount to disenchantment. Today, for many who invest political hopes in cryptography, the transformation of a message into random characters through cryptography aligns with a political stance in which the natural world, treated as an extra-human space, may provide refuge from the state, or even serve the functions at which the state has apparently failed. Digital security experts are fond of illustrating the strength of modern cryptography with dramatic comparisons to the natural world. To break a message encrypted with a typical, widely available algorithm (TK-bit AES) would require enough energy to boil all the water in all the world's oceans. Even using the most powerful computer available today, this would take TK million years.

Hence the powerful allure of the cryptographic sublime to cyber-libertarians, crypto-anarchists, and others attracted to the idea of fashioning new, perhaps freer societies on foundations of digital technology.[15]

The image of nature as a quasi-mystical refuge has a long history in the American imagination, but so does the image of technology as a force to shape these essentially empty landscapes into civilization. For early European settlers, the new continent was

[15] Turner, Fred. From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism. Chicago: University of Chicago Press, 2006.

alternately interpreted as an Eden untouched by the evils of mankind, or as a savage, god-forsaken land that required taming. Henry David Thoreau found the solace of the forest momentarily defiled whenever a train would pass on the rail line near Walden Pond, its steam whistle puncturing the natural environment that he imagined as a pristine refuge from the ills of civilization several miles up the road. The historian Leo Marx identifies this duality as a defining force in the construction of American culture, and he defines the experience of the technological sublime as a union of the two.[16] David Nye identifies the great bridges, dams, and skyscrapers as iconic sources of the technological sublime in American experience. When these structures do provoke feelings of the sublime, they may "represent a way to reinvest the landscape and the works of men with transcendent significance."[17]

Now consider Snowden and Assange, who appeal to the universal laws of nature as a source of both transcendent awe and mechanical certainty in cryptography. They are as transfixed with the cryptographic sublime as any mystic who sees the divine in coded texts or inscrutable symbols hidden in the natural world. In this sense, the cryptographic sublime is nothing new, and it is certainly not limited to the privacy and transparency activists who are most vocal about cryptography's fundamental importance today. The political affordances ascribed to cryptography stand as some of the most peculiar features of its mythos. Cryptography is credited with the power to marshal resistance against forces that are otherwise unassailable. It is trusted not only to guard the world of online finance, but also to secure a growing share of mundane web

[16] Marx, Leo. "The Machine in the Garden." *The New England Quarterly* 29, no. 1 (March 1956): 27.

[17] Nye, David E. *American Technological Sublime*. Cambridge, Mass: MIT Press, c1994, p. xiii.

traffic that is routinely monitored as it traverses the global internet. When encrypted, transmissions become a scrambled mess of characters, unreadable without the corresponding decryption key. Whereas breathless accounts of the digital revolution amid its onset once implied immanent transcendence beyond the restrictions of the physical world — promising limitless dissemination of information,[18] disembodied virtual experience,[19] even post-scarcity economics[20] — cryptography has been effective at placing limits on digital utopian fantasies, readily contradicting some of the qualities once considered definitive of 'the digital' by the first wave of writers associated with the cyberculture.[21] Crypto makes information unreadable, placing barriers in the so-called 'cyberspace' that had once been portrayed as an ideal, boundless realm of pure information. The widespread use of crypto today reflects something different: a desire to place limits on information, reasserting conditions of the physical world we are accustomed to living within. Crypto can set barriers to protect against eavesdropping, and it is often used to block access to copyrighted content, much like television channels that were once scrambled for non-subscribers. Crypto can hide identifying information, offering anonymity, but it can also also be used to verify information using

[18] Barlow, J.P. "Selling Wine Without the Bottles," in Ludlow, ed. *Crypto-Anarchy, Cyberstates, and Pirate Utopias*.

[19] Lanier, Jaron, and Frank Biocca. "An Insider's View of the Future of Virtual Reality." Journal of Communication 42, no. 4 (December 1, 1992): 150–72.

[20] Stallman, Richard, "GNU Manifesto," in *The Manifesto in Literature*, 3:355–57, 2013.

[21] John Perry Barlow and Nicholas Negroponte are representative proponents of this stance. See Barlow, "Declaration of the Rights of Cyberspace" and Negroponte's *Being Digital* (199x).

digital signatures.[22] It is trusted to undersign such apparently unforgeable objects as cryptocurrency. Likewise, the digital ledgers known as blockchains, designed to prevent duplicate spending of cryptocurrency, are currently in the midst of fevered proliferation as a means of documenting and verifying all manner of digital transactions — essentially as a new means of doing old forms of business. If the dream of the early Internet would be a post-scarcity world, unencumbered by physical limits, so far cryptography has proved to be a reliable means of replacing and securing limits, barriers, and other assurances that digital information will continue to be a rivalrous good. Snowden's principal cause, for instance, is to reestablish rights that have apparently eroded in the digital age. Noble as the cause may be, it is not a progressive vision of a new world. Snowden wants to maintain or even return to a past state of affairs. Assange, on the other hand, views cryptography as a tool to weaponize secrecy, undermine established regimes of power, and presumably to liberate humanity from state oppression. Cryptography did not appear to have any such potential a century ago, nor even fifty years ago, and these five chapters describe a series of historical phases in which cryptography has undergone progressive transformation — from art to science, from handwriting to computation, from mere puzzle solving to fierce political clashes over the right to privacy.

Chapter 1, "Cryptography and Written Culture" calls attention to a wide array of uses, both systematic and unsystematic, that the increasingly literate American public

[22] For a study of the legal status of digital signatures, see Jean-François Blanchette's *Burdens of Proof: Cryptographic Culture and Evidence Law in the Age of Electronic Documents*. Cambridge, Mass: MIT Press, 2012.

found for cryptography during the nineteenth and early twentieth century. During this time, secret codes and ciphers were a common feature of print and written culture, including letters, diaries, puzzles, fiction, and commerce. On the other hand, the American government and military had remarkably little interest in cryptography until after the turn of the twentieth century, contrary to the myth that the right to use cryptography has only recently been ceded to the American public in light of an extraordinary need for information security in the digital age. Instead, much of what constituted the broad popular interest in cryptography a century ago would only begin to be excluded through boundary work after the 1920s, as systematic, scientific approaches to cryptography began to be placed at the center of focus, with non-scientific approaches increasingly marginal. And yet some handwritten codes remain resilient against computational codebreaking — underlining that the apparent universality of digital information leaves a set of marginal practices that have not yet been subsumed to this other logic.[23]

In Chapter 2, "Communication and its Limits," I examine the scientific view of cryptography that took shape with the emergence of information theory, statistical approaches to language, and digital communications in the first half of the twentieth century. There were several competing early versions of information theory, but Claude Shannon's was unique in its presentation of the 'noise' in electrical communications as a controllable, even useful phenomenon. This perspective grew out of Shannon's

[23] Although a computer vision program tailored for handwriting recognition could feasibly cover some distance in breaking handwritten codes, it would still be more computationally complex and unreliable than breaking a purely digital code through brute force guessing by a computer that knows the exact set of discrete combinations for exhaustive checking.

assignment to work on cryptography during World War II, leading him to frame communication and cryptography as merely different ways of coding a transmission, whether to preserve the signal against the noise, or to give the appearance of noise to potential eavesdroppers or 'enemies'. Although these terms — 'signal' and 'noise' — are commonly taken to mean something like 'good information' and 'bad information', Shannon offered a subtler mode of understanding noise than many of his peers. Shannon viewed the distinction between signal and noise as essentially contingent, context-dependent, ultimately a matter of agreement between the sender and receiver of a particular message using a particular code. This is a largely unrecognized point of difference between Shannon and his contemporaries who were working on the same problem, but this point would form the basis of later thinking about cryptography as an artful use of noise, which may be shifted to signal through coding.

Shannon's flexible stance on noise came after a long period of progressive, incremental changes in the perception of noise by his predecessors. To recognize the usefulness of noise in communication and cryptography stems from a shift in scientific thinking that Ian Hacking has called 'taming of chance', essentially pointing to the rise of probability and statistics in the nineteenth century. Hacking tracks the gradual appreciation of randomness as something both fundamental and useful in math, science, and engineering. The paradoxical implications of this shift would form the basis of the scientific definition of information that emerged in the first half of the twentieth century. Noise was slowly recognized as something controllable, often through technology, and this formed the basic insights underlying Shannon's mathematical theories of communication and cryptography. It is these peculiar 'laws of

nature' that many cryptographers invoke today when they describe the remarkable qualities of modern cryptography, although the scientific view of cryptography described in this chapter was not yet invested with politics. That would come later. The essentially apolitical Shannon viewed his work, and especially his work for the military, in a starkly different light than those who would later treat cryptography as a tool for social change.

Chapter 3, "Classifying Cryptography," observes the postwar moment when cryptography began to be strictly controlled by the American government, legally defined as a weapon, and research in the subject treated as a matter of utmost secrecy. This chapter departs from the moment when Shannon published his theories of communication and cryptography in quick succession after the end of World War II. His crypto paper was declassified in 1949, a full twelve years ahead of the declassification schedule stamped on its cover page. This gesture of openness would turn out to be a peculiar but telling outlier: his communication theory of cryptography was the last substantial piece of research published for a quarter century on this subject, although it still remained little noticed compared to his theory of communication.

Although many historical accounts treat cryptography as the sole, longstanding purview of government, it was only in the postwar years that the American government planted a firm claim upon research into codes and ciphers. In the early years of the Cold War, espionage and fears of espionage had been a source of escalated geopolitical tensions, and the Soviet Union's apparent acquisition of technical plans to build nuclear weaponry instigated calls for heightened security in military research — an institution that was carried forward after the war at the urging of many American

military leaders, research administrators, and intelligence agents leading the newly established CIA and NSA. Largely as a consequence of increased urgency surrounding espionage and intelligence work, cryptography, writ large, continued to be treated as a classified research subject even after armistice. The Cold War powers would practice espionage even more intensely than they had during the war. Before cryptography would even gained its footing as an area of scientific study, at least openly, cryptography was named in international arms treaties as a weapon in itself and regulated alongside nuclear physics. A number of prominent American scientists publicly appealed for greater openness in scientific research, in general, arguing that persistent classification in peacetime would be out of step with the open, democratic ideals they had come to consider essential to the very endeavor of science.[24] For the NSF's founding director, Vannevar Bush, this ideological tension was a remarkable source of doublespeak: Bush outwardly promoted a vision of a thriving open society, driven by scientific progress, but he also worked to keep a great many areas of scientific knowledge secret, including cryptography.

For a quarter century beginning in the early nineteen fifties, cryptography research would be conducted mostly in secret, sometimes in universities, but not disclosed publicly. Much of this research was managed by the newly established NSA, who would seek out the expertise of mathematicians like Shannon and Von Neumann for cryptographic advisory groups to offer expert consultation with difficult problems. Overall, this chapter examines the moment when cryptography became entangled with

[24] See Audra J. Wolfe's *Freedom's Laboratory: The Cold War Struggle for the Soul of Science*. Baltimore: Johns Hopkins University Press, 2018.

a growing culture of secrecy that was typically justified by grave political concerns in the postwar period — the struggles of oppositional superpowers and the threat of nuclear annihilation. The result was a certain amnesia washing over the longer history of social roles for cryptography that were described in Chapter 1, as well as a general suppression of research on cryptography, stifling recognition of Shannon's work on cryptography even as information theory and computer science progressed rapidly through the 1950s and 60s. This amnesia is palpable in the following chapter.

Chapter 4, "Thinking About Information Security in the 1960s," looks at concerns about the rise of computing and threats to privacy rights expressed in American political discourse during the sixties, with particular attention to the fact that cryptography was largely absent from discussion. The concerns that motivated researchers to work in cryptography a decade later in fact emerged into conversation during the 1960s. This chapter is a case study centered on a 1966 proposal to establish a 'National Data Bank' (NDB) to gather information from across the US government in a central computer database, promising efficiency gains and better access to data for economic planning — but also prompting a furious backlash from many politicians and legal scholars, as well as broadly negative press coverage and public sentiment about the implications of this proposal, often expressed in literally Orwellian terms.

The timing of the proposal for a federal database of statistical data on individual citizens was historically significant: following the recent passage of the Freedom of Information Act (FOIA), opponents of the NDB were driven by a related but distinct interest in the growing cultural ideal of transparency. Several congressmen said the various offices of the federal government may already collect too much information

about citizens, and a centralized computer system could lead to even greater potential for the mismanagement of this information. In short, whereas FOIA promised the general public access to government information in light of the fact that more and more was being collected, opponents of the NDB treated it as a measure that could strengthen the negative effects of the data gathering itself. These hearings echoed growing concerns about information security and privacy as projections of the coming computer age began to percolate through American society. Many of the concerns voiced about privacy and computer security in 1966 carry on today, over fifty years later, in roughly the same language. And yet, even though this debate evinces a prescient grasp of looming concerns, the ultimate answer could seem naive to many privacy advocates today: there was broad agreement that access restrictions and legal penalties could help curtail abuses by federal employees with access to so much sensitive information. Cryptography was only briefly mentioned as a possible countermeasure, and quickly dismissed as too expensive. In short, the postwar suppression of cryptography left the field essentially stagnant and forgotten among the general American public from the 1940s through the 1960s, and the only mention of cryptography in the NDB hearings came from Paul Baran, an employee of the defense contractor Rand Corporation who had drawn up the original plan for the Arpanet three years earlier.

The case of the NDB proposal reveals that cryptography was essentially absent from consideration, even in a discussion explicitly centered on computers and invasion of privacy. Still, much of the rhetoric of today's cryptography advocates had already entered the discourse by this time, as a rising interest in transparency and distrust of

government secrecy was already taking shape in the broader culture. In short, the postwar suppression of cryptography research left the field essentially stagnant and mostly forgotten through the 1960s, even as concerns about computers and privacy began to enter serious conversation about technological changes and social hazards for the society to come. The strict classification of cryptography would have the unexpected effect of amplifying and politicizing efforts to research this subject in the open during the 1970s, commingling the liberation of cryptography research with the social concerns that led to this liberation, a subject addressed in the next chapter.

Chapter 5, "Cryptography's Public Reemergence," examines the moment when cryptography ceased to be strictly classified, amid a gradual wave of change that included both compromises and outright dissent. Although NSA held a tight grip on cryptography research until the late 1960s, this loosened when they granted IBM a highly limited exception, and this inch expanded to the proverbial mile when other researchers refused to honor official requests to keep the matter classified. The move was nevertheless bold, and the purpose of this chapter is to examine the greater cultural context that motivated these researchers to behave so boldly. Moreover, I examine the political and social factors that enabled them to succeed. In short, efforts to conceal cryptography research during the post-war years became untenable by the seventies amid broader shifts in the politics of information: growing disapproval of government secrecy, the ascent of transparency as a cultural value, and heightened expressions of concern about electronic surveillance, whether in centralized computer databases or over nascent networks that were projected to connect computers all over the globe. The computer scientists who chose to pursue open cryptography research

did so against the warnings of their colleagues, as well as a series of threats stating that any public discussion of cryptography research would be a felony violation of international arms treaties. They continued this research nonetheless, and justified their decision to pursue public studies of cryptography on several distinct grounds: their belief in free speech, opposition to secrecy in science, the promise of discovery, a competitive desire for peer recognition, as well as a conviction that cryptography would soon become a subject of manifest importance for the protection of privacy in the information age.

The common element in this laundry list of motivations is that cryptography researchers in the seventies were pushing for transparency, in a broad sense, and pushing against official secrecy. The reemergence of cryptography research can be productively understood as a post-Watergate, post-Pentagon Papers development, prompted by the growing sense that the public both has a general 'right to know' and a specific prerogative to distrust appeals to government secrecy. This is one of the key moments when cryptography began to be treated as a tool of political resistance, social change, and specifically as a ward against invasion of privacy through electronic surveillance. Although a series of legal standoffs in the nineties (often called the 'Crypto Wars') tend to be recognized as the formative moment for the politics of cryptography today, the seventies actually marked the moment when the Snowden-Assange view of cryptography coalesced, binding computational wizardry to oppositional politics.

This also points to a distinct, separate genesis for the identification of cryptography as a 'liberation technology,' a claim often attached to computers and digital media more generally. The distinct historical origin of cryptography's current politics underlines a

critical contrast with the liberatory claims associated with the main branch of digital politics, an ethos traced by Fred Turner from the sixties counterculture through the emergence of the nineties counterculture.[25] Digital utopians promoted computers and the Internet as tools that could liberate us by granting unbridled access to information, limitless interconnection to others worldwide, and unfettered access to public platforms for speech. Cryptography's politics are grounded on opposite principles: placing barriers on information access, securing information from exposure, protecting sensitive personal information, and ensuring the possibility of private conversation. Cryptography is not a tool of digital utopianism. Instead, we might think of its ethos as counter-utopian, in much the same way that Isaiah Berlin identified a counter-enlightenment in which the principles of the Romantic era gestated as a distinct stream of thought that only emerged in full cultural flourish at a later date. The optimism of the early digital age has been tested, tempered, even undermined over time, the counter-utopian ethos expressed by Snowden, in particular, has become a more convincing political stance, and it is worth recognizing its historical origins not in the sixties counterculture or the nineties cyberculture, but in the culture of transparency and anti-secrecy in the seventies.

The reemergence of cryptography research in the seventies was also the source of cryptography's current scientific paradigm, which was grounded on the rediscovery of Shannon's cryptographic theory from a quarter century earlier and a rapid succession of revisions that pulled this theory up to speed with developments from the intervening

[25] Turner, Fred. *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*. Chicago: University of Chicago Press, 2006.

years. Shannon attracts a peculiar cult of personality, much like others ascribed credit for founding entire fields of study, not least when they are credited with 'inventing' the present age. What's most remarkable about Shannon's theory of cryptography, paired with his broader theory of information, is that it provides the building blocks for both the digital utopian framing of the information age, and the alternative that has been cultivated around cryptography. His theory of communication grounds the possibility of limitless, flawless telecommunication using digital computers; his theory of cryptography explains how to use essentially the same coding principles to limit information access to only certain audiences. Cryptography itself is an often vexing concept, difficult to define and prone to harboring contradictions. For instance, although cryptography is a means of communication, it is distinguished by its capacity to block communication. A tool of secrecy, it is increasingly placed in the service of transparency. A tool of obfuscation, it may also be used to verify information. Cryptographic communication has always been accomplished by creating symbolic barriers, using the sources of communication's failure as a means of controlling access to messages, but with the computer age came new affordances for secret codes. The formal study of cryptography today is grounded in computation, and even though the history of cryptography evinces many computational precursors to current methods, the opening chapter examines a broader cross-section of methods for both concealing messages and seeking hidden messages during the age of print, before cryptographic communication carried either the scientific or political commitments that characterize it today.

Conclusion

In 2014, a hacker conference in New York City bridged several generations of whistleblowers when they billed their keynote address as a conversation between Daniel Ellsberg and Edward Snowden — albeit with Snowden coming through on a video screen, dialed in from exile in Moscow. While Ellsberg's own work in the sixties had been decidedly 'offline', its most sophisticated technological point being the use of a photocopier, in recent years Ellsberg had become a vocal advocate of digital encryption as a means of ensuring that future whistleblowers could safely share information with reporters. The two also share an affiliation through the Freedom of the Press Foundation, where Ellsberg was a co-founder and remains a board member, while Snowden now acts as the organization's president. The FPF's main project, at least through its early years, has been to develop and proliferate an encrypted whistleblowing platform specifically designed for newsrooms called SecureDrop. This project stands as a clear example of the "over-engineered solutions" that Snowden described in his early emails with Poitras as a means of resisting mass surveillance through "the laws of nature rather than the laws of man."

The connection between these two whistleblowers goes deeper, as I argued in Chapter 5. For the groundswell of opposition to official secrecy by Ellsberg and others in the early seventies also aided the contemporaneous push for open research on cryptography, not to mention bolstering the argument for its necessity as a safeguard of private information. I have argued that without whistleblowers like Ellsberg to blow open state secrets, without reporters like Seymour Hersh to drive more aggressive reporting, and without an intense series of Congressional investigations from 1971-4, digital cryptography would have taken a very different shape than it has today.

The scientific principles underlying cryptography have settled into a stable paradigm since the seventies, the locus of cryptography proper firmly centered on the principles of information theory, itself rooted in the spread of probability and statistics throughout the natural and social sciences. Modern cryptography requires vast reserves of random, but more often pseudorandom numbers produced by purpose-built algorithms. The encrypted message takes on the appearance of noise, just as random as thermodynamic motion or radioactive decay. Nevertheless, these are treated as natural phenomena, grounded in physics, undersigned by mathematics, and thus they could seem to stand apart from humanity or the social world even as they are treated as socially transformative technologies.

For Snowden, Assange, and the cypherpunks, the entropy in nature is both a resource and a transcendent ideal in itself. Entropy represents a natural force apparently working in their favor, or at least a ready resource for developing technology with these values baked in. To recognize the usefulness of a force so apparently chaotic as entropy, or so apparently destructive as electrical noise, required

a counterintuitive and often misunderstood theoretical leap during the formation of information theory in the 1940s, a subject outlined in Chapter 2. The transcendent perfection invested in cryptography descends initially from the work of Claude Shannon, but follows through the rediscovery of his work in the seventies and the development of even more stunning mathematical perfections in the development of trapdoor functions like RSA, which offer an asymmetrical advantage to the encrypter.

Yet the scientific foundations of modern, computational cryptography cannot explain the social and political ethos invested in cryptography as a vehicle of counter-power, which Manuel Castells calls "one of the few natural laws of society" and defines as "the capacity by social actors to challenge and eventually change the power relations institutionalized in society."[385] Whether or not counter-power is really a natural law of society,' cryptography has only recently emerged as an apparent form of counter-power. As I argue in Chapter 1, cryptography was not freighted with political significance before the twentieth century. In Chapter 3, I describe a period beginning in the 1940s when the United States government began to strictly control cryptography research during a dramatic rise in official secrecy, while Chapter 5 locates the origins of cryptography's current political commitments only in the 1970s, when the newly emergent field was essentially a tabula rasa to be imprinted with the ethos of the time. Recalling the passages quoted above, Snowden and Assange take it as given that modern cryptography is a lever of popular resistance, a natural force to undermine

[385] Castells, Manuel. "Communication, Power and Counter-Power in the Network Society," International Journal of Communication 1 (2007), p. 248.

domination, whether to hold our ground or to reshape the political landscape. It is a messy fusion of political, metaphysical, and aesthetic commitments. Assange, in particular, reveals a taste for the esoteric, promising arcane knowledge and power through cryptography. This tendency to marvel at the wondrous, distant, even fearsome power of cryptography carries the essential qualities of the sublime. To believe a message is perfectly inscrutable to human reason can make it appear boundless, even beautiful. An unreadable wall of text may inspire awe, wonder, even a hint of uneasiness. Like hieroglyphs, which once provided a deep reserve of fantasy precisely because they could potentially mean anything at all, decipherment is tantamount to disenchantment. Today, for many who invest political hopes in cryptography, the transformation of a message into random characters through cryptography aligns with a political stance in which the natural world, conceived as an extra-human space, may provide refuge from the state. For proponents of widespread public access to strong cryptography, it is treated as the mortar ensuring the structural integrity of the digital world. Backdoors, built-in weaknesses, and other compromises to the strength or soundness of modern cryptography have come to be treated as anathema, with even a Congressional task force in the nineties asserting cryptography's essential role in securing the information society.

Still, beyond cryptography's advocates and reluctant allies, others remain wary of widespread public access to encryption. The strength of cryptography that is celebrated by Snowden and Assange is treated as a threat by those who would prefer, in a manner of speaking, for the 'laws of nature' not to overtake the 'laws of man'. The former FBI director James Comey, for instance, has described the power of modern cryptography

as a fearsome tool in the hands of criminals, terrorists, and other villains. Echoing a failed campaign to institute 'key escrow' technology in the nineties, Comey and others have pushed for tech companies to include 'backdoors' that would allow law enforcement access to encrypted messages in the course of their investigations. By and large, tech companies tend to be unwilling to poke holes in their own security. Most have not complied with official requests to weaken their encryption, and through a combination of both active and passive adoption, a steadily increasing share of all web traffic is now transmitted using some form of encryption. In short, those pushing for weaker crypto are faced instead with more and stronger crypto. Former Director of National Intelligence James Clapper reported that whistleblowers have had a measurable impact on the trend of increasing cryptography use among the general public. "As a result of the Snowden revelations, the onset of commercial encryption has accelerated by seven years," Clapper said, adding that this has hampered their pursuit of terrorists. When asked if the resulting security benefits for average citizens could be treated as a positive outcome, Clapper said: "From our standpoint, it's not … it's not a good thing."[386] Losing ground, the transcript suggests fatigue, and as more tech companies continue build cryptography into their products by default, the sides are shifting by fiat as cryptography is increasingly enmeshed with everyday life.

Today, among advocates of digital security, cryptography is treated as a means to safeguard individual liberty, privacy, and the freedom of the press; to facilitate free

[386] McLaughlin, Jenna. "Spy Chief Complains That Edward Snowden Sped Up Spread of Encryption by 7 Years." *The Intercept* (blog), April 25, 2016.

markets; to check or even undermine the reach of government. And yet, cryptography was not invested with such strong political associations until very recently, despite its long history. A century ago, cryptography was neither framed as a science, nor treated as political, nor even claimed by the US government as its sovereign jurisdiction. Although cryptography can be traced deep into antiquity, and a variety of methods for concealing writing have proliferated across culture, codes and ciphers haven't carried the weight of safeguarding liberty until very recently, with the earliest examples in this study appearing in the 1970s. I argue in Chapter 5 that cryptography could not have become invested with such deep political commitments if it hadn't been suppressed in research and the media during the postwar years. The greater the force exerted to dissuade writers and scientists from studying cryptography, the more the subject became wrapped in the luminous aura of civil disobedience. The tone that surrounded the reemergence of crypto in the 1970s was one of urgent public need. It was a stance of dissent, part of a greater groundswell that traveled out of the social movements of the sixties. Yet this protest was distinct as an early case of computer experts stepping in to protect the public from dangers on the horizon of the coming information age. Unlike any other branch of mathematics or computer science, cryptography is embedded in social life, and many of the figures who have gravitated to cryptography since its reemergence have viewed their work as inherently political.

As I argue in Chapter 4, one of the major factors that enabled a cohort of computer scientists to reopen cryptography research in the 1970s was a uniquely tumultuous moment in Washington politics, when demands for transparency reached a fever pitch and official secrecy was placed under the microscope. With the Pentagon Papers,

Watergate, and a stream of aggressive, ambitious investigative journalism, the US government suffered a series blows in the public eye that increasingly aligned public opinion with the antiwar movement of the sixties. Many Americans had grown skeptical of government secrecy, in general, and intelligence agencies in particular. The disclosure of the Pentagon Papers had validated many of the concerns voiced by antiwar protesters throughout the 1960s. The collapse of the Nixon administration amid the Watergate investigation suggested that even the president could not be trusted to use his powers justly. The hearings of the Church and Rockefeller committees pried open the clandestine operations of the CIA and NSA to reveal not only ethically questionable practices, but also programs that violated US law, international law, and the agencies' respective charters. This string of revelations in the early 1970s marked a moment when the need to protect state secrets began to appear suspicious to many Americans, including elected officials. Meanwhile the growing demand for legislation to protect privacy rights culminated in the Privacy Act of 1974, which requires government agencies to issue public notice of the information it gathers about private individuals, and prohibits disclosure of information without an individual's written consent.[387]

By the mid 1970s, concerns about privacy and government transparency had come to outweigh the case for secrecy that had once seemed justified during the early years of the Cold War and the rapid growth of the intelligence community. The computer scientist Martin Hellman points to this volatile political moment in the post-Watergate

[387] Privacy Act of 1974, 5 U.S.C. § 552a. Available online at https://www.justice.gov/opcl/privacy-act-1974.

era as a factor that motivated him and his collaborators to work on new cryptography methods in defiance of restrictions placed on this subject. Although he and his collaborators received numerous warnings and even threats, they were adamantly opposed to secrecy, especially in science. And as the senior figure in a cohort leading the reemergence of research in this field, Hellman was in a position of considerable leverage to place Shannon at the core of the field, even as he revised and updated Shannon's work to account for developments in the field of information science during the intervening years. Since then, Shannon's work has been treated as the conceptual origin of modern cryptography even though this work was utterly obscure and totally unused by computer scientists for twenty-five years after it was published. The rediscovery and promotion of Claude Shannon's cryptographic theory in the 1970s was driven by Hellman's own scholarly investment in Shannon's better known work, the mathematical theory of communication. That is, Hellman worked in a field where Shannon's related work had already been established as canonical. It was straightforward for Hellman to read this obscure paper from 1949, grasp its neglected significance, and use it as a lens for entirely new and groundbreaking work. Hellman critiqued and revised the weaknesses that had arisen in the intervening decades, but for the most part Hellman deserves credit for claiming Shannon as a father of modern cryptography after Shannon's work on this subject had been mostly ignored for decades.

When researchers campaigned to publish on the subject of cryptography in the 1970s, they justified their work on political grounds and discussed it in public forums. Hellman sent op-eds to various newspapers to convey his position to the public, asking

for cryptography's public need to be reassessed by politicians as well as officials at the agencies resisting his right to publish. Advocates of cryptography and the broader field of computer security in the 1960s and 70s actively reframed these subjects and promoted them as a means of guarding the boundary between the public and private sphere in the information age.

These emergent political investments in cryptography have since become standard lines among civil libertarians (like Edward Snowden and the EFF), radical transparency activists (like Julian Assange and other hacktivists), computer scientists (among whom cryptographers are still some of the most politically active), and journalists (who increasingly use encryption tools to communicate with sources). This dissertation outlines the sources of narratives and other cultural forms that frame cryptography today, as well as sources of conspicuous omission in cryptographic history. Cryptography has become distinctly political, even radical over the last century, but the history of this subject is still poorly developed, narrow in scope, and out of sync with the broader field of social studies of science and technology. Historians of cryptography have not reckoned with social constructionism or actor-network theory. They have not faced postcolonial, feminist, or even Marxist critique. A field that has persisted with such consistency amid vigorous changes in scholarly conversation could be considered the definition of an intellectual backwater, and this is particularly unfortunate given the political stakes surrounding cryptography today. A critical history of cryptography should be skeptical of linear progress narratives, inquiring into the social factors that shaped the field, and always asking what's missing from the story.

History often turns on momentous coincidences, illustrating the "social significance of statistically insignificant events," as Michael Schudson puts it. When historians are able to identify those critical events and traces the forking paths through time, what emerges is a "record of events moving people and institutions irretrievably in this direction and not that one."[388] Some events are chancy, improbably hinging on an apparent twist of fate, while others may be determined or even overdetermined by forces like social movements, media narratives, policy, commerce, or the emergence of new technologies. Still, some events push us toward certain outcomes, precluding others, forming a path-dependent sequence, and our understanding of the past is itself a force in the present.

In light of the developments outlined in these chapters, it would be more accurate and charitable to the history of cryptography for a distinction to be made between techniques for computational cryptography and other techniques, which do not rely on algorithmic transformations of text but on some other way of concealing communications. Today, non-computational means of concealing a message or its contents tend to be accepted only as historical precursors of cryptography proper. This is a bit like saying that an old wooden bridge is only technically a bridge, and if you built a bridge like that today it really wouldn't be a bridge at all. It could be unwise to direct a city's rush-hour traffic over a wooden bridge built with carts and horses in mind, and it is a genuinely impressive feat of engineering for modern bridges to remain secure under so much force. The sophistication of computational cryptography is similarly impressive. When assailed through brute force, modern cryptography remains resilient

[388] Michael Schudson, *Watergate in American Memory* (New York: Basic Books, 1992), p. 1.

even against the onslaught of today's supercomputers, an asymmetrical advantage to the defender. The same clever math forms the foundation underlying cryptocurrency. But still it is an error to grant computational forms of cryptography sole, paradigmatic privilege, drawing a boundary that excludes techniques that cannot be fitted to Shannon's schema. For Shannon's very definition of cryptography insists on the assumption that 'the enemy knows the system,' disqualifying any form of steganography, or hiding messages. Many pre-digital codes have yet to be cracked, from manuscripts written in eccentric, invented shorthand, to undeciphered ancient scripts like Linear B.[389]

Perhaps the most common trope in writings on the history of cryptography is to gesture toward its ancient origins, typically with passing reference to places like Egypt or Babylon, often punctuated with the claim that the invention of cryptography nearly always follows shortly after the invention of writing itself. The trouble with this trope is not that it's inaccurate, nor unsupported, nor even unimportant, but rather that authors seem to deploy it with the intention of establishing cryptography's deep, long-standing connection to the broader history of communication, but unfailingly abandon any deeper inquiry into these connections. Let us not assume that privacy and secrecy are

[389] Several linguists have found success recently using computational methods to decipher manuscripts written in unknown symbols, but their work rests heavily on their own ability to form hypotheses about the potential structure of the code in question before they build a computational model to test this hypothesis. For instance, Rajesh Rao of the University of Washington has used statistical analysis, markov models, and entropic evidence in an effort to decode the script of the ancient Indus River Valley civilization. For a representative paper, see Rao, Rajesh P. N. "Probabilistic Analysis of an Ancient Undeciphered Script." Computer 43, no. 4 (April 1, 2010): 76.

the inevitable motives of cryptography. If the next question is ‘why?’ then the conversation often turns reductive, often with an appeal to human nature, living side-by-side in settlements, discovering the affordances of written communication. I leave this study most convinced of a realization I reached in Chapter 1: the reasons for writing in codes and ciphers could very well be limitless, and the narrow conception of cryptography as one set of practices or another has impoverished our understanding. The difference between written language, code, and cipher breaks down quickly under examination, leading to the variety of legal argument posed by Moglen when he says that the right to ‘speak PGP’ is like the right to speak Navajo. This is the same fuzzy distinction that has made codebreaking techniques historically useful for deciphering ancient languages, as well as scanning the cosmic background radio noise for the possibility of alien signals. The root assumption is that the sense, the signal, something nonrandom will emerge. And yet, in the most difficult cases, it is noise that gathers the greatest scrutiny, which holds the greatest fascination, and this is the basis of the cryptographic sublime — what in the digital age may plausibly undersign our rights and liberties more soundly than the law itself. The more ubiquitous cryptography becomes, the more this claim may become grounded as a social fact, true if only because it is built into the infrastructure that organizes social life.